UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

PI-EQUIVALÊNCIA EM ÁLGEBRAS GRADUADAS SIMPLES

Fernando Augusto Naves

SÃO CARLOS - SP

2016

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

PI-Equivalência em Álgebras Graduadas Simples

Fernando Augusto Naves

Orientador: Prof. Dr. Humberto Luiz Talpo

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

SÃO CARLOS - SP

2016

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária UFSCar
Processamento Técnico
com os dados fornecidos pelo(a) autor(a)

Naves, Fernando Augusto
N323p PI-equivalência em álgebras graduadas simples / Fernando Augusto Naves. -- São Carlos : UFSCar, 2016.
88 p.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2016.

1. PI-Álgebras. 2. G-graduações. 3. Identidades polinomiais. 4. Identidades graduadas. 5. Álgebras graduadas simples. I. Título.

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Fernando Augusto Naves, realizada em 29/02/2016:

Prof. Dr. Humberto Luiz Talpo
UFSCar

Thiago Castilho de Mello

Prof. Dr. Thiago Castilho de Mello
UNIFESP

Dimas José Gonçalves

Prof. Dr. Dimas Jose Goncalves
UFSCar

Agradecimentos

A Deus, que se faz presente em minha vida, guiando meus passos e concedendo-me graças a cada dia.

À Universidade Federal de São Carlos (UFSCar), em especial ao Departamento de Matemática (DM).

Ao meu orientador Humberto Luiz Talpo, pela imensa atenção, disponibilidade e ajuda durante todo o período do mestrado. Seus ensinamentos, que foram além da matemática em si, foram fundamentais para meu crescimento pessoal e profissional. Deixo meu mais sincero agradecimento por ter me orientado.

Aos professores do DM, pelos valiosos ensinamentos, em especial ao professor Dimas por ter dado importantes contribuições a este trabalho e à minha formação.

A todos os amigos que fiz aqui em São Carlos, os quais carrego no coração. Decido não enumerá-los para não cometer a injustiça de esquecer de alguém.

À minha mãe, pessoa mais inteligente que já conheci, a quem devo tudo do pouco que sou. Todos os seus ensinamentos foram as coisas mais inportantes que aprendi na vida.

Ao meu pai por me ensinar o valores de honestidade, caráter, e hombridade.

À minha irmã, uma das minhas maiores incentivadoras desde sempre.

À minha esposa Priscilla pelo apoio incondicional, pela paciência e por fazer com que meus dias fossem mais alegres. Nada disso seria possível sem seu amor.

Aos meus primos Hilda e Wilmar que me acolheram em São Carlos da melhor maneira possível.

À CAPES pelo suporte financeiro.

A todos que contribuíram direta ou indiretamente.

Se, depois de eu morrer, quiserem escrever a minha biografia,
Não há nada mais simples.
Tem só duas datas - a da minha nascença e a da minha morte.
Entre uma e outra cousa, todos os dias são meus.
(Fernando Pessoa)

Resumo

Este trabalho tem por objetivo dar uma descrição, sob certas hipóteses, das álgebras graduadas simples e demonstrar que elas são determinadas por suas identidades graduadas. Para isso, estudamos os artigos [3] e [19]. Precisamente mostraremos o seguinte: sejam G um grupo, F um corpo algebricamente fechado e $R = \bigoplus_{g \in G} R_g$ uma F-álgebra G-graduada de dimensão finita, tal que a ordem de todo subgrupo finito de G é invertível em F. Então R é uma álgebra G-graduada simples se, e somente se, R é isomorfa, como álgebra graduada, ao produto tensorial $C = M_n(F) \otimes F^{\sigma}[H]$, onde H é subgrupo finito de G, σ é um 2-cociclo em H, $M_n(F)$ tem uma graduação elementar, $F^{\sigma}[H]$ tem uma graduação canônica e considera-se em C a G-graduação induzida pelo produto tensorial. Partindo deste resultado, admitindo as mesmas hipóteses e adicionando que G seja um grupo abeliano, provaremos que duas álgebras graduadas simples satisfazem as mesmas identidades graduadas se, e somente se, são isomorfas como álgebras graduadas.

Palavras Chave: *PI-Álgebras, G-graduações, Identidades Polinomiais, Identidades Graduadas, Álgebras Graduadas Simples.*

Abstract

This work aims to give a description, under certain hypothesis, of the graded simple algebras and prove that they are determined by their graded identities. For this, we study the papers [3] and [19]. More precisely we will show the following: Let G be a group, F an algebraically closed field, and $R = \bigoplus_{g \in G} R_g$ a finite dimensional G-graded F-algebra such that the order of each finite subgroup of G is invertible in F. Then R is a G-graded simple algebra if and only if R is isomorphic, as graded algebra, to the tensor product $C = M_n(F) \otimes F^\sigma[H]$, where H is a finite subgroup of G, σ is a 2-cocycle in H, $M_n(F)$ has an elementary G-grading, $F^\sigma[H]$ has a canonical grading and C has an induced G-grading by the tensor product. Based on this result, admitting the same assumptions and adding that G is an abelian group, we prove that two graded simple algebras satisfy the same graded identities if and only if they are isomorphic as graded algebras.

Keywords: *PI-Algebras, G-gradings, Polynomial Identities, Graded Identities, Graded Simple Algebras.*

Sumário

Introdução

Dizemos que um polinômio $f(x_1, \ldots, x_n)$ em variáveis não comutativas $x_1, \ldots, x_n$ é uma *identidade polinomial* para uma álgebra R (ou que R satisfaz a identidade f) se $f(r_1, \ldots, r_n) = 0$ para quaisquer elementos $r_1, \ldots, r_n \in R$. Uma álgebra que satisfaz uma identidade polinomial não nula é chamada de *PI-álgebra*. Por exemplo, se R é uma álgebra comutativa então $x_1x_2 - x_2x_1$ é uma identidade polinomial não nula para R. É possível mostrar com facilidade que as álgebras nilpotentes e as de dimensão finita também são PI-álgebras. Por outro lado, existem álgebras que não satisfazem nenhuma identidade não nula. Sendo assim, o estudo da classe das PI-álgebras engloba muitas outras classes de álgebras, tal como as comutativas, as nilpotentes e as de dimensão finita. Esta é uma área da Álgebra, mais especificamente da teoria de anéis e álgebras, bastante ativa ainda nos dias de hoje.

Podemos considerar que o estudo de PI-álgebras começou com os trabalhos de Dehn [8] e Wagner [27] nas décadas de 20 e 30. Porém foi com os trabalhos de Kaplansky [17] em 1948 e de Amitsur e Levistky [2] em 1950 que houve um maior desenvolvimento dessa área. Em [2] apareceu o famoso teorema de Amitsur-Levitzki que afirma que o polinômio *standard*

$$st_{2n}(x_1, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} (-1)^{\sigma} x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n)}$$

é uma identidade polinomial para $M_n(F)$. Em [10] há duas demonstrações distintas deste resultado. Para mais informações sobre o desenvolvimento do estudo de PI-álgebras, indicamos [13], [21], [10] e [26].

Muitas questões surgem do estudo das PI-álgebras. Por exemplo: seja F um corpo e denote por $F\langle X \rangle$ a álgebra dos polinômios nas variáveis não comutativas $\{x_1, x_2, \ldots\}$ com coeficientes em F. Considere uma F-álgebra arbitrária R e denote por $T(R)$ o conjunto de todas as identidades polinomiais de R, que será um T-ideal de $F\langle X\rangle$, isto é, $T(R)$ é invariante por endomorfismos de $F\langle X\rangle$. É possível encontrar um subconjunto finito de $F\langle X\rangle$ que determina o mesmo T-ideal $T(R)$? Mais do que isso: é possível explicitar uma base para as identidades de uma dada álgebra? Comentamos brevemente a respeito desses problemas na seção 2.1. Indicamos [10] e [26] para mais informações.

Frequentemente, o uso de uma graduação em uma álgebra é uma ferramenta importante na obtenção de resultados. Essa situação nos leva às noções de polinômio graduado, identidade polinomial graduada e isomorfismo graduado. Aliás esse tipo de abordagem aparece no célebre artigo de Kemer [18] no qual ele apresenta uma resposta afirmativa ao problema de Specht, quando a característica do corpo é zero.

Um outro problema interessante, porém complicado e amplo é o seguinte: a partir do conhecimento (parcial ou não) das identidades(graduadas) de uma álgebra(graduada) R, que propriedades gerais R possui? Por exemplo, se R é uma álgebra associativa não unitária sobre um corpo de característica 0 satisfazendo uma identidade do tipo x^k, isto é, R é uma nil álgebra com índice limitado, então o teorema de Nagata-Higman garante a existência de um inteiro d, dependendo de k, tal que R é nilpotente com índice de nilpotência d.

Vamos nos ater neste trabalho a um caso "específico" da seguinte questão: sejam duas F-álgebras(graduadas) A e B tais que A e B satisfazem as mesmas identidades(graduadas). Qual a relação entre A e B? Já é sabido que se duas álgebras são isomorfas então elas satisfazem as mesmas identidades polinomiais. Porém, sabe-se que a recíproca não é necessariamete verdadeira, isto é, se duas álgebras satisfazem as mesmas identidades polinomiais então não são necessariamente isomorfas. Mostramos isso no exemplo 2.1.17. Então é naturalmente levantada a questão: Existe alguma "classe" de álgebras em que seus elementos são determinados, a menos de isomorfismo, pelas identidades satisfeitas? A resposta é sim e é isso a razão principal deste trabalho. Nós estaremos interessados no caso das álgebras graduadas. Mostraremos que se duas álgebras graduadas simples satisfazem as mesmas identidades graduadas então elas são isomorfas, impondo algumas hipóteses sobre a dimensão dessas álgebras, sobre o grupo que as gradua e sobre o corpo base. Nesse sentido, o artigo de Aljadeff e Haile [1] generaliza o resultado de Koshlukov e Zaicev [19] sem usar como hipótese que o grupo seja abeliano. O trabalho está organizado em quatro capítulos da seguinte maneira:

O primeiro capítulo aborda os conceitos preliminares necessários à leitura do texto. Revemos os conceitos de álgebra, subálgebra e ideal de uma álgebra. Apresentamos exemplos desses entes matemáticos de modo conveniente à nossa necessidade posterior. Abordamos também a definição de produto tensorial de módulos, espaços vetoriais e álgebras, discutindo de forma breve suas propriedades mais importantes. Além disso, também falamos sobre o produto tensorial de aplicações lineares entre módulos. Algumas das afirmações feitas nesse capítulo estão sem demonstração, mas indicamos onde podem ser encontradas.

O segundo capítulo diz respeito às álgebras graduadas e identidades polinomiais. Na seção 2.1 definimos com rigor as noções de álgebra livre, variedade de álgebras, polinômio, identidade polinomial e PI-álgebra. Novamente, os exemplos apresentados foram muitas vezes escolhidos de forma a podermos retomá-los quando necessário. Faremos também uma breve discussão sobre o problema de Specht com indicação de alguns resultados clássicos a respeito. Na seção 2.2 definimos o importante conceito de álgebra graduada e mostramos alguns exemplos de graduações em certas álgebras específicas que serão usadas no segmento do trabalho. Já na seção 2.3 definimos o conceito de polinômio graduado e identidade polinomial graduada, que serão as identidades com as quais, de fato, trabalharemos.

O terceiro capítulo refere-se primordialmente aos resultados de Bathurin, Zaicev e Sehgal [3]. Na seção 3.1 mostraremos que as álgebras graduadas simples sobre um corpo arbitrário F são necessariamente unitárias. Na seção 3.2 descreveremos todas as álgebras graduadas de divisão de dimensão finita sobre um corpo algebricamente fechado. Na seção 3.3 provamos que se R é uma álgebra G-graduada simples de dimensão finita sobre um corpo algebricamente fechado F de tal sorte que a ordem de cada subgrupo finito de G seja invertível em F então R é semissimples. E finalmente na seção 3.4 descreveremos todas as F-álgebras G-graduadas simples de dimensão finita impondo certas condições sobre o corpo F e o grupo G. Esta última seção é inteiramente dedicada à demonstração do teorema de descrição, que foi dividida em lemas e resultados preliminares de modo a tornar a prova mais construtiva.

O quarto e último capítulo, inspirado no resultado principal do capítulo anterior, é dedicado a demonstrar o resultado principal da dissertação, que é o fato de que as F-álgebras G-graduadas simples (com certas hipóteses sobre o corpo F, sobre o grupo G e sobre a dimensão de R) são determinadas, a menos de isomorfismo graduado, pelas suas identidades graduadas. O resultado se refere ao artigo de Koshlukov e Zaicev [19], embora por vezes usamos a abordagem dada por Aljadeff e Haile [1].

Capítulo 1

Pré-requisitos

Neste capítulo definiremos os principais conceitos e apresentaremos os principais resultados que necessitaremos no desenvolvimento do trabalho. Para mais detalhes e aprofundamento dos conceitos indicamos [12], [15] e [16].

1.1 Preliminares

Nesta seção, sempre que mencionado F denotará um corpo qualquer.

Definição 1.1.1. *Seja A um F-espaço vetorial. Diremos que A é uma **F-álgebra** se existe uma operação $*: A \times A \to A$ tal que para quaisquer $\alpha \in F$ e $a, b, c \in A$ valem:*

1. $(a + b) * c = a * c + b * c$;

2. $a * (b + c) = a * b + a * c$;

3. $\alpha(a * b) = (\alpha a) * b = a * (\alpha b)$.

*Neste caso diremos que $*$ é um **produto** (ou multiplicação) em A. Usualmente escrevemos ab no lugar de $a * b$. Diremos que:*

1. *A é **associativa** se $a(bc) = (ab)c$ para quaisquer $a, b, c \in A$;*

2. *A é **comutativa** se $ab = ba$, para quaisquer $a, b \in A$;*

3. *A é* ***unitária*** *se existe um elemento $1_A \in A$ tal que $1_A a = a 1_A = a$, para qualquer $a \in A$ (denotamos 1_A por 1, desde que não se confunda tal elemento com a identidade do corpo F);*

4. *A é uma* ***álgebra de divisão*** *se todo elemento não nulo de A é invertível em A;*

5. *A é uma* ***álgebra de Lie*** *se para quaisquer $a, b, c \in A$ valem:*

$$a^2 = 0,$$
$$(ab)c + (bc)a + (ca)b = 0 \text{ (Identidade de Jacobi).}$$

Exemplo 1.1.2. *O conjunto dos números reais com as operações usuais é uma $\mathbb{R}$-álgebra de divisão, comutativa, associativa e unitária.*

Exemplo 1.1.3. *O espaço vetorial $M_n(F)$ é uma F-álgebra associativa e unitária.*

Exemplo 1.1.4. *O espaço vetorial $\mathbb{R}^3$ é uma $\mathbb{R}$-álgebra de Lie, considerando o produto vetorial $\times$ usual em $\mathbb{R}^3$.*

Definição 1.1.5. *Sejam A uma F-álgebra e S um subespaço vetorial de A. Então*

1. *S é dito ser uma* ***subálgebra*** *de A se S for fechado com relação ao produto de A;*

2. *S é dito ser um* ***ideal à esquerda*** *de A se*

$$as \in S$$

   para quaisquer $a \in A$ e $s \in S$;

3. *S é dito ser um* ***ideal à direita*** *de A se*

$$sa \in S$$

   para quaisquer $a \in A$ e $s \in S$.

4. *Se S for simultaneamente um ideal à esquerda e à direita de A então dizemos que S é um* ***ideal bilateral*** *de A (ou simplesmente ideal de A).*

Exemplo 1.1.6. *Seja A uma F-álgebra associativa. Então pode-se definir um novo produto em A, dado por*

$$\begin{aligned} [\ ,\ ] : A \times A &\longrightarrow A \\ (a,b) &\longmapsto [a,b] := ab - ba. \end{aligned}$$

O F-espaço vetorial A munido deste novo produto é uma álgebra de Lie e a denotamos por $A^{(-)}$. É bem sabido que toda álgebra de Lie L é isomorfa a uma subálgebra de uma álgebra $R^{(-)}$, para alguma álgebra associativa R. Essa é uma das consequências do teorema de Poincaré-Birkhoff-Witt, que pode ser encontrado em [10].

Exemplo 1.1.7. *Seja V um F-espaço vetorial com base ordenada*

$$B = \{e_i \ : i \in I\}.$$

A ***Álgebra de Grassmann (ou exterior) E(V)*** *de V é a álgebra associativa unitária gerada (como álgebra) pelo conjunto B que satisfaz*

$$e_i e_j = -e_j e_i$$

para todos $i, j \in I$ e também

$$e_i^2 = 0 \text{ se } char(F) = 2.$$

Tal álgebra existe. De fato, considere o conjunto de variáveis $X = \{x_i \ : i \in I\}$. Seja J o ideal em $F\langle X\rangle$ gerado pelos polinômios

$$x_i x_j + x_j x_i, \text{ onde } i, j \in I.$$

Então $E(V) \cong \frac{F\langle X\rangle}{J}$.

Exemplo 1.1.8. *O conjunto $U_n(F)$ das matrizes triangulares superiores é uma subálgebra de $M_n(F)$.*

Exemplo 1.1.9. *O subespaço S de $U_n(F)$ formado pelas matrizes com diagonal principal* *nula é um ideal de $U_n(F)$.*

Exemplo 1.1.10 (Centro de uma álgebra)**.** *Dada uma álgebra A, definimos o **centro** de A como sendo o conjunto*

$$Z(A) := \{z \in A \ : za = az, \ \forall a \in A\}.$$

Não é difícil ver que $Z(A)$ é uma subálgebra de A. Por exemplo, temos que

$$Z(M_n(F)) = \{\lambda I_n \ : \lambda \in F\}$$

onde I_n é a matriz identidade $n \times n$.

Definição 1.1.11. *Sejam A e B duas F-álgebras. Uma aplicação $\varphi : A \to B$ é um **homomorfismo de álgebras** se φ é uma transformação linear e se*

$$\varphi(aa') = \varphi(a)\varphi(a')$$

*para quaisquer $a, a' \in A$. Se além disso φ for bijetora então dizemos que φ é um **isomorfismo de álgebras**. Duas F-álgebras A e B são ditas **isomorfas** se existe um isomorfismo de álgebras $\varphi : A \to B$. Neste caso denotamos $A \cong B$.*

Sejam A uma F-álgebra e J um ideal de A. Então o F-espaço vetorial quociente $\frac{A}{J}$ é uma F-álgebra com produto

$$\overline{a}\overline{a'} = \overline{aa'},$$

onde $\overline{a} = a + J$. A F-álgebra $\frac{A}{J}$ é chamada de **álgebra quociente**. A proposição a seguir é o teorema do isomorfismo para álgebras, cuja demonstração é análoga à que é feita no teorema do isomorfismo para anéis:

Proposição 1.1.12. *Seja $\varphi : A \to B$ um homomorfismo de álgebras. Então o conjunto*

$$Ker(\varphi) := \{a \in A \ : \varphi(a) = 0\},$$

*chamado de **núcleo de** φ é um ideal de A e*

$$\frac{A}{Ker(\varphi)} \cong Im(\varphi).$$

Para finalizar a seção, fica essa proposição que será útil no futuro:

Proposição 1.1.13. *Seja D uma álgebra de divisão de dimensão finita sobre um corpo algebricamente fechado F. Então $D \cong F$.*

Demonstração. Denote por 1 a unidade de D. Defina $\varphi : F \to D$ dada por $\varphi(\alpha) = \alpha 1$. Observe que φ é um homomorfismo injetor de F-álgebras. Mostremos que $\varphi(F) = D$.

Para cada $d \in D$, defina $f_d : D \to D$ por $f_d(x) = xd$. Observe que f_d é um homomorfismo de D-módulos e também é F-linear. Suponha que exista $a \in D$ mas $a \notin \varphi(F)$. Fixe uma base ordenada $B = \{u_1, \ldots, u_n\}$ de D. Denote a matriz de f_a em relação à base B por $[f_a]_B$. Como F é algebricamente fechado, seja $\lambda \in F$ um autovalor de $[f_a]_B$. Considere agora a aplicação

$$f_{a-\lambda 1} : D \to D.$$

Não é difícil ver que $[f_{a-\lambda 1}]_B = [f_a]_B - \lambda I_n$, onde I_n é a matriz identidade em $M_n(F)$. Como λ é raiz do polinômio $det([f_a]_B - xI_n)$, temos que $f_{a-\lambda 1}$ não é um isomorfismo. Como D é um D-módulo simples, devemos ter $f_{a-\lambda 1}$ identicamente nula. Daí

$$0 = f_{a-\lambda 1}(1) = a - \lambda 1$$

o que implica que $a = \lambda 1 \in \varphi(F)$, uma contradição. Isso termina a proposição. □

1.2 Produto tensorial

Nesta seção faremos a parte introdutória a respeito do produto tensorial para desenvolver as ferramentas necessárias no decorrer do texto. Não nos debruçaremos sobre todas as propriedades do produto tensorial, mas somente àquelas que nos interessam ao desenvolvimento do trabalho. Para mais detalhes, indicamos [12].

1.2.1 Produto tensorial de módulos, espaços vetoriais e álgebras

Os anéis considerados neste capítulo serão sempre com unidade. Sempre que não mencionado nesta seção, R representará um anel e o termo R-módulo significará R-módulo à esquerda.

Definição 1.2.1. *Sejam M e N dois R-módulos. Denote por $F_{M\times N}$ o R-módulo livre gerado pelo conjunto $M \times N$, isto é, todas as combinações lineares formais, com coeficientes em R, de elementos do tipo $(m,n) \in M \times N$. Tome agora H como o submódulo de $F_{M\times N}$ gerado por todos os elementos da forma*

$$\begin{aligned}(m_1+m_2,n)-(m_1,n)-(m_2,n)\\ (m,n_1+n_2)-(m,n_1)-(m,n_2)\\ (rm,n)-(m,rn)\\ r(m,n)-(rm,n)\\ r(m,n)-(m,rn),\end{aligned}$$

*com $r \in R$, $m, m_1, m_2 \in M$ e $n, n_1, n_2 \in N$. O R-módulo quociente $\frac{F_{M\times N}}{H}$ recebe o nome de **produto tensorial de** M **por** N e é denotado por $M \otimes N$. Denotamos a classe contendo (m,n) em $M \otimes N$ por $m \otimes n$.*

Observe que pelas relações acima, para quaisquer $r \in R$, $m, m_1, m_2 \in M$ e $n, n_1, n_2 \in N$, valem as relações:

$$\begin{aligned}(m_1+m_2)\otimes n &= m_1\otimes n + m_2 \otimes n\\ m\otimes(n_1+n_2) &= m\otimes n_1 + m\otimes n_2\\ r(m\otimes n) &= (rm)\otimes n = m\otimes(rn)\end{aligned}$$

Cada elemento da forma $m\otimes n \in M\otimes N$ recebe o nome de **tensor simples**. Observe que cada elemento de $M \otimes N$ é uma combinação linear de tensores simples.

Proposição 1.2.2. *Sejam I e J dois conjuntos de índices e M e N dois R-módulos gerados por $\{x_i\}_{i\in I}$ e $\{y_j\}_{j\in J}$, respectivamente. Então o conjunto*

$$\{x_i \otimes y_j \ : i \in I, j \in J\}$$

gera $M \otimes N$.

Demonstração. Um tensor simples em $M \otimes N$ é da forma $m \otimes n$. Escreva $m = \sum_i a_i x_i$ e $n = \sum_j b_j y_j$, onde os coeficientes $a_i, b_j \in R$ são todos nulos, exceto por uma quantidade finita. Assim, pela bilinearidade do produto tensorial

$$m \otimes n = \left(\sum_i a_i x_i\right) \otimes \left(\sum_j b_j y_j\right) = \sum_{i,j} a_i b_j \left(x_i \otimes y_j\right).$$

Como todo tensor de $M \otimes N$ é um combinação linear de tensores simples, segue a proposição. $\square$

Como $M \otimes N$ é um quociente, é preciso tomar cuidado ao definir funções cujo domínio é $M \otimes N$. O próximo teorema é imporante para tal tarefa. Antes de enunciá-lo, precisamos da definição:

Definição 1.2.3. *Sejam M, N e P R-módulos. Uma aplicação $g : M \to N$ é dita ser **linear** se*

$$g(rm_1 + m_2) = rg(m_1) + g(m_2)$$

*para quaisquer $r \in R$, $m_1, m_2 \in M$. Uma aplicação $f : M \times N \to P$ é dita ser **bilinear** se*

$$f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n), \quad f(rm, n) = rf(m, n)$$
$$f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2), \quad f(m, rn) = rf(m, n)$$

para quaisquer $r \in R$, $m, m_1, m_2 \in M$ e $n, n_1, n_2 \in N$.

Teorema 1.2.4 (Propriedade universal)**.** *Considere a aplicação bilinear natural $i : M \times N \to M \otimes N$ dada por $i(m, n) = m \otimes n$. Então, dada uma aplicação bilinear $f : M \times N \to L$, onde L é um R-módulo, existe uma única aplicação linear $\widetilde{f} : M \otimes N \to L$ tal que o seguinte diagrama comuta*

$$\begin{tikzcd} M \otimes N \arrow[rd, dotted, "\widetilde{f}"] & \\ M \times N \arrow[u, "i"] \arrow[r, "f"'] & L \end{tikzcd} \tag{1.2.1}$$

Mais do que isso: existe uma bijeção entre $Bil(M \times N; L)$ *e* $Hom(M \otimes N; L)$ *com respeito à comutatividade do diagrama* (1.2.1).

Demonstração. Como $F_{M\times N}$ é livre sobre $M \times N$, podemos estender f para uma função linear $g : F_{M\times N} \to L$ tal que $g((m,n)) = f((m,n))$. Mostremos que H (dado pela definição 1.2.1) está contido em $Ker(g)$. Usando a bilinearidade de f e a linearidade de g temos que

$$g((m_1+m_2,n)) = f((m_1+m_2,n)) = f((m_1,n)) + f((m_2,n)) = g((m_1,n)) + g((m_2,n))$$
$$g((m,n_1+n_2)) = f((m,n_1+n_2)) = f((m,n_1)) + f((m,n_2)) = g((m,n_1)) + g((m,n_2))$$
$$g((rm,n)) = f((rm,n)) = rf((m,n)) = f((m,rn)) = g((m,rn))$$
$$g(r(m,n)) = rg((m,n)) = rf((m,n)) = f((rm,n)) = g((rm,n)) = g((m,rn))$$

para quaisquer $r \in R$,, $m, m_1, m_2 \in M$ e $n, n_1, n_2 \in N$. Assim, g se anula nos geradores de H, isto é, $H \subset Ker(g)$. Deste modo, g induz uma aplicação linear $\widetilde{f} : F_{M\times N}/H \to L$ dada por $\widetilde{f}(m \otimes n) = g(m,n) = f(m,n)$, o que significa que o diagrama 1.2.1 comuta. Mostremos agora a unicidade da aplicação $\widetilde{f}$ quanto à comutatividade do diagrama 1.2.1. Suponha que $\alpha : M \otimes N \to L$ seja outra aplicação linear tal que 1.2.1 comuta. Deste modo, dado $u \in M \otimes N$, temos que

$$u = r_1(m_1 \otimes n_1) + \cdots + r_k(m_k \otimes n_k)$$

para certos $r_i \in R$, $m_i \in M$ e $n_i \in N$. Assim,

$$\begin{aligned} \alpha(u) &= \sum_{i=1}^{k} r_i \alpha(m_i \otimes n_i) \\ &= \sum_{i=1}^{k} r_i f(m_i, n_i) \\ &= \sum_{i=1}^{k} \widetilde{f}(r_i(m_i \otimes n_i)) \\ &= \widetilde{f}(u), \end{aligned}$$

como queríamos demonstrar. Para a recíproca, o argumento é análogo. $\square$

Exemplo 1.2.5. *Seja A um grupo abeliano qualquer tal que todo elemento de A tem ordem finita. Então podemos ver A e $\mathbb{Q}$ como dois $\mathbb{Z}$-módulos. Afirmamos que $\mathbb{Q} \otimes A = 0$. De fato, dado $a \in A$, seja $n \in Z$ tal que $na = 0$. Assim, para qualquer $r \in \mathbb{Q}$, tem-se*

$$r \otimes a = n(r/n) \otimes a = r/n \otimes na = r \otimes 0 = 0.$$

Assim, todo tensor elementar é nulo, o que mostra que $\mathbb{Q} \otimes A = 0$.

Exemplo 1.2.6. *Para inteiros positivos a, b, seja $d = mdc(a, b)$. Então $\mathbb{Z}/a\mathbb{Z} \otimes \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$. Em particular, $\mathbb{Z}/a\mathbb{Z} \otimes \mathbb{Z}/b\mathbb{Z} \cong 0$ se, e somente se, $d = 1$.*

O produto tensorial pode ser estendido para mais de dois fatores. Dados n R-módulos $M_1, \ldots, M_n$, existe um R-módulo $M_1 \otimes \cdots \otimes M_n$ que cumpre a propriedade universal: dada uma aplicação n-multilinear $f : M_1 \times \cdots \times M_n \to L$, existe uma única aplicação linear $\widetilde{f} : M_1 \otimes \cdots \otimes M_n \to L$ tal que o seguinte diagrama comuta

$$\begin{tikzcd}
M_1 \otimes \cdots \otimes M_n \arrow[dr, dotted, "\widetilde{f}"] & \\
M_1 \times \cdots \times M_n \arrow[u, "i"] \arrow[r, "f"'] & L
\end{tikzcd}$$

Tal módulo pode ser construído de maneira similar através de um quociente do R-módulo livre $F_{M_1 \times \cdots \times M_n}$.

Teorema 1.2.7. *Sejam M e M' dois R-módulos livres com bases $\{e_i \ : i \in I\}$ e $\{e'_j \ : j \in J\}$, respectivamente. Então $M \otimes M'$ tem base $\{e_i \otimes e'_j \ : i \in I, j \in J\}$.*

Demonstração. Pela proposição 1.2.2, $\{e_i \otimes e'_j \ : i \in I, j \in J\}$ gera $M \otimes M'$. Tome agora a combinação linear $\sum_{i,j} c_{ij} e_i \otimes e'_j = 0$, onde todos c_{ij}, exceto por uma quantidade finita, são nulos. Escolha arbitrariamente dois índices $i_0 \in I$ e $j_0 \in J$. Defina a aplicação bilinear (verifique !) $f : M \times M' \to R$ dada por $f(u, v) = u_{i_0} v_{j_0}$, se $u = \sum_i u_i e_i$ e $v = \sum_j v_j e'_j$. Pela propriedade universal, existe uma aplicação $\widetilde{f} : M \otimes M' \to R$ tal que $\widetilde{f} \circ i(u, v) = f(u, v)$, para todo $u, v \in M \times M'$, isto é, $f(u \otimes v) = u_{i_0} v_{j_0}$. Em particular, $\widetilde{f}(e_{i_0} \otimes e'_{j_0}) = 1$ e $\widetilde{f}(e_i \otimes e'_j) = 0$ se $(i, j) \neq (i_0, j_0)$. Aplicando $\widetilde{f}$ à equação $\sum_{i,j} c_{ij} e_i \otimes e'_j = 0$, obtemos $c_{i_0 j_0} = 0$, terminando o teorema. $\square$

Cabe notar que se U e V são dois F-espaços vetoriais, podemos fazer a mesma "construção" para falar em produto tensorial de U e V, começando com o espaço vetorial livre $F_{U\times V}$ e passando ao quociente por um subespaço análogo ao definido inicialmente. A propriedade universal do teorema 1.2.4 se mantém válida para o caso de espaços vetoriais.

Exemplo 1.2.8. *Seja V um F-espaço vetorial. Então pelo teorema anterior $F \otimes V \cong V$.*

Exemplo 1.2.9. *Sejam x, y duas variáveis comutativas e considere o R-módulo $R[x, y]$. Observe que $\{x^i y^j \ : i, j \geq 0\}$ é uma base para $R[x, y]$. Como $R[x]$ tem base $\{x^i \ : i \geq 0\}$ e $R[y]$ tem base $\{y^j \ : j \geq 0\}$ então $R[x] \otimes R[y] \cong R[x, y]$.*

Teorema 1.2.10. *Existe um único isomorfismo de R-módulos $\widetilde{f} : M \otimes N \to N \otimes M$ tal que $\widetilde{f}(m \otimes n) = n \otimes m$.*

Demonstração. Defina $f : M\times N \to N\otimes M$ por $f(m, n) = n\otimes m$. Observe que f é bilinear. Pela propriedade universal, existe uma única aplicação linear $\widetilde{f} : M\otimes N \to N\otimes M$ tal que $\widetilde{f}(m\otimes n) = n\otimes m$, para todos $m \in M, n \in N$. De modo absolutamente análogo, mostra-se que existe uma única aplicação linear $g : N \otimes M \to M \otimes N$ tal que $g(n \otimes m) = m \otimes n$, para todos $n \in N, m \in M$. Mostremos que $\widetilde{f}, g$ são inversas uma da outra.

Para mostrar que $\widetilde{f} \circ g = Id$, basta checarmos em tensores simples (uma vez que $\widetilde{f}$ e g são lineares). Mas isso é imediato, bem como $g \circ \widetilde{f} = Id$. Portanto $\widetilde{f}$ é um isomorfismo de R-módulos. □

O produto tensorial de módulos tem "boas" propriedades. Abaixo enunciamos dois teoremas que mostram esse fato. Para as demonstrações, consulte [12].

Teorema 1.2.11. *Existe um único isomorfismo de R-módulos $\widetilde{f} : (M \otimes N) \otimes P \to M \otimes (N \otimes P)$ tal que $\widetilde{f}((m \otimes n) \otimes p) = m \otimes (n \otimes p)$.*

Teorema 1.2.12. *Seja I um conjunto de índices. Existe um único isomorfismo de R-módulos*

$$\widetilde{f} : M \otimes \bigoplus_{i\in I} N_i \longrightarrow \bigoplus_{i\in I}(M \otimes N_i)$$

tal que $\widetilde{f}(m \otimes (n_i)_{i\in I}) = (m \otimes n_i)_{i\in I}$.

1.2.2 Produto tensorial de aplicações e de álgebras

Sejam M, M', N, N' R-módulos e $\varphi : M \to M'$ e $\psi : N \to N'$ duas aplicações lineares. Então podemos definir uma aplicação $\varphi \times \psi : M \times N \to M' \otimes N'$ dada por $(\varphi \times \psi)(m, n) = \varphi(m) \otimes \psi(n)$. Como φ e ψ são lineares, segue que $\varphi \times \psi$ é bilinear. Pela propriedade universal, existe uma aplicação

$$\varphi \otimes \psi : M \otimes N \to M' \otimes N'$$

tal que $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$, para todos $m \in M, n \in N$. A aplicação $\varphi \otimes \psi$ é chamada de **produto tensorial de φ e ψ**. O produto tensorial de aplicações pode ser concebido no contexto de espaços vetoriais e de álgebras.

Proposição 1.2.13. *Sejam R-módulos M e N. Então $id_M \otimes id_N = id_{M\otimes N}$. Para aplicações lineares $\varphi : M \to M'$, $\varphi' : M' \to M''$, $\psi : N \to N'$ e $\psi' : N' \to N''$,*

$$(\varphi' \otimes \psi') \circ (\varphi \otimes \psi) = (\varphi' \circ \varphi) \otimes (\psi' \circ \psi)$$

como aplicações lineares de $M \otimes N$ em $M'' \otimes N''$.

Demonstração. A aplicação $id_M \otimes id_N$ é uma aplicação linear de $M \otimes N$ em $M \otimes N$ que fixa todo tensor elementar. Então ela fixa todos os tensores.

Como $(\varphi' \otimes \psi') \circ (\varphi \otimes \psi)$ e $(\varphi' \circ \varphi) \otimes (\psi' \circ \psi)$ são aplicações lineares, para provar a igualdade é suficiente provar que coincidem em um tensor simples qualquer $m \otimes n$, que ambas assumem o valor $\varphi'(\varphi(m)) \otimes \psi'(\psi(n))$. □

O seguinte teorema está enunciado para módulos mas tem o análogo para espaços vetoriais e álgebras:

Teorema 1.2.14. *Se $\varphi : M \to M'$ e $\psi : N \to N'$ são isomorfismos de R-módulos, então $\varphi \otimes \psi : M \otimes N \to M' \otimes N'$ é um isomorfismo de R-módulos*

Demonstração. Basta ver que $\varphi\otimes\psi$ e $\varphi^{-1}\otimes\psi^{-1}$ são R-lineares e inversas uma da outra. □

Proposição 1.2.15. *Se $\varphi : M \to M'$ e $\psi : N \to N'$ são sobrejetoras então $\varphi \otimes \psi$ é sobrejetora.*

Demonstração. Como $\varphi \otimes \psi$ é linear, basta mostrar que todo tensor elementar de $M' \otimes N'$ está na imagem de $\varphi \otimes \psi$. Para cada $m' \otimes n' \in M' \otimes N'$, escreva $m' = \varphi(m)$ e $n' = \psi(n)$. Daí, $m' \otimes n' = \varphi(m) \otimes \psi(n) = \varphi \otimes \psi(m \otimes n)$. □

Um aspecto do produto tensorial de aplicações é que o produto de aplicações injetoras não é necessariamente injetora, como vemos no exemplo:

Exemplo 1.2.16. *Tome $R = \mathbb{Z}$ e considere $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}$ dada por $\alpha(x) = px$, para todo $x \in \mathbb{Z}/p\mathbb{Z}$. Considere também a aplicação identidade $Id : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Observe que α e Id são $\mathbb{Z}$-homomorfismos injetores. Assim, obtemos a aplicação*

$$Id \otimes \alpha : \mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}/p^2\mathbb{Z}$$

que satisfaz

$$x \otimes y \mapsto x \otimes py = px \otimes y = 0.$$

Assim, $Id \otimes \alpha$ é identicamente nula e seu domínio é $\mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \neq 0$, então $Id \otimes \alpha$ não é injetora.

Nesse sentido, como o produto tensorial de aplicações não preserva a injetividade, não é necessariamente verdade que se $M \subset M'$ e $N \subset N'$ então o produto tensorial $M \otimes N$ é submódulo de $M' \otimes N'$, uma vez que a aplicação natural $M \otimes N \to M' \otimes N'$ não é necessariamente injetora.

Exemplo 1.2.17. *Note que $p\mathbb{Z} \cong \mathbb{Z}$ como grupos abelianos, através da aplicação $pn \mapsto n$. Assim, $\mathbb{Z}/pZ \otimes p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$ como grupos abelianos através da aplicação $a \otimes pn \mapsto a \otimes n \mapsto na \text{ mod } p$. Observe agora que $1 \otimes p \in \mathbb{Z}/pZ \otimes pZ$ é não nulo pois é identificado com $1 \in \mathbb{Z}/p\mathbb{Z}$. Porém, $1 \otimes p$ é nulo em $\mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}$ pois $1 \otimes p = 1 \otimes p1 = p \otimes 1 = 0 \otimes 1 = 0$. Pode parecer estranho que $1 \otimes p$ é não nulo em $\mathbb{Z}/pZ \otimes p\mathbb{Z}$ enquanto que $1 \otimes p$ é nulo em $\mathbb{Z}/pZ \otimes \mathbb{Z}$. A razão de tal fato é que $\mathbb{Z}/pZ \otimes p\mathbb{Z}$ não é subgrupo (e portanto não é submódulo) de $\mathbb{Z}/pZ \otimes \mathbb{Z}$, ainda que $p\mathbb{Z}$ seja um subgrupo de $\mathbb{Z}$.*

A aplicação inclusão $i : p\mathbb{Z} \to \mathbb{Z}$ nos fornece uma aplicação natural $Id \otimes i : Z/pZ \otimes p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \otimes Z$ dada por $(Id \otimes i)(a \otimes pn) = a \otimes pn$. Porém tal aplicação não é um mergulho. De fato, sua imagem é nula em $\mathbb{Z}/p\mathbb{Z} \otimes Z$ pois $a \otimes pn = pa \otimes n = 0 \otimes n = 0$. O ponto chave é que $a \otimes pn$ tem significados diferentes em $\mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}$ e $\mathbb{Z}/p\mathbb{Z} \otimes p\mathbb{Z}$

O próximo resultado, nos garante que o produto tensorial de duas álgebras é ainda uma álgebra:

Proposição 1.2.18. *Sejam A e B duas F-álgebras. Considere o espaço vetorial $A \otimes B$. Então a multiplicação $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$ está bem definida e torna $A \otimes B$ uma F-álgebra.*

Demonstração. Inicialmente, pela propriedade universal e pela bilinearidade da multiplicação em A e B, podemos definir as aplicações F-lineares $m_A : A \otimes A \longrightarrow A$ e $m_B : B \otimes B \longrightarrow B$ tais que $m_A(a \otimes a') = aa'$ e $m_B(b \otimes b') = bb'$. Então o produto tensorial das aplicações $m_A \otimes m_B$ é uma aplicação F-linear de $(A \otimes A) \otimes (B \otimes B)$ em $A \otimes B$. Usando os isomorfismos de comutatividade e associatividade do produto tensorial, temos

$$\begin{aligned}
(A \otimes B) \otimes (A \otimes B) &\cong ((A \otimes B) \otimes A) \otimes B) \\
&\cong (A \otimes (B \otimes A)) \otimes B \\
&\cong (A \otimes (A \otimes B)) \otimes B \\
&\cong ((A \otimes A) \otimes B) \otimes B \\
&\cong (A \otimes A) \otimes (B \otimes B).
\end{aligned}$$

Usando os efeitos desses isomorfismos em um tensor simples $(a \otimes b) \otimes (a' \otimes b')$,

$$\begin{aligned}
(a \otimes b) \otimes (a' \otimes b') &\mapsto ((a \otimes b) \otimes a') \otimes b') \\
&\mapsto (a \otimes (b \otimes a')) \otimes b' \\
&\mapsto (a \otimes (a' \otimes b)) \otimes b' \\
&\mapsto ((a \otimes a') \otimes b) \otimes b' \\
&\mapsto (a \otimes a') \otimes (b \otimes b').
\end{aligned}$$

Compondo esses isomorfismos com $m_A \otimes m_B$, obtemos uma aplicação F-linear $f : (A \otimes B) \otimes (A \otimes B) \to A \otimes B$ que tem o efeito

$$(a \otimes b) \otimes (a' \otimes b') \mapsto aa' \otimes bb'.$$

Assim, a aplicação

$$\widetilde{f} : (A \otimes B) \times (A \otimes B) \to A \otimes B$$

dada por $\widetilde{f}(a \otimes b, a' \otimes b') = f((a \otimes b) \otimes (a' \otimes b')) = aa' \otimes bb'$ é linear e está bem definida, pois f o está. Essa aplicação determina uma aplicação bilinear

$$(A \otimes B) \times (A \otimes B) \longrightarrow A \otimes B$$

com efeito

$$(a \otimes b, a' \otimes b') \longmapsto aa' \otimes bb'.$$

Portanto $A \otimes B$ é uma F-álgebra. □

Corolário 1.2.19. *Se A e B são duas F-álgebras comutativas então $A \otimes B$ é uma F-álgebra comutativa*

Demonstração. Imediato. □

Capítulo 2

Álgebras graduadas e identidades polinomiais

O conceito de álgebras graduadas é uma ferramenta muito utilizada na Matemática. Nesta seção daremos os conceitos e propriedades iniciais do assunto, dando enfoque nas álgebras e graduações que nos serão úteis mais à frente. Para mais informações, indicamos [3], [4] e [10]. Sempre que mencionarmos, F será um corpo qualquer.

2.1 Álgebras livres, identidades polinomiais e variedades

Definição 2.1.1. *Seja $\mathfrak{U}$ uma classe de álgebras e seja $A \in \mathfrak{U}$ uma álgebra gerada por um conjunto X. A é dita ser uma* ***álgebra livre na classe $\mathfrak{U}$, livremente gerada por*** *X, se para qualquer $R \in \mathfrak{U}$, toda aplicação $f : X \to R$ puder ser estendida a um homomorfismo de álgebras*

$$\overline{f} : A \to R.$$

A cardinalidade $|X|$ é chamada de ***posto de*** *A.*

Considere um conjunto qualquer X. Uma **palavra** sobre X é uma concatenação de elementos

$$x_{i_1} \cdots x_{i_n},$$

onde $x_{i_j} \in X$ e $n \in \mathbb{N} \cup \{0\}$. A "palavra vazia"(quando $n = 0$) será denotada por 1. Considere o F-espaço vetorial $F\langle X\rangle$ cuja base é formada por todas as palavras sobre X, isto é, todo elemento de $F\langle X\rangle$ é uma combinação linear formal, com coeficientes em F, de palavras sobre X. Podemos definir a seguinte multiplicação entre duas palavras e depois estender por linearidade o produto para quaisquer dois elementos de $F\langle X\rangle$:

$$(x_{i_1} \cdots x_{i_n})(x_{j_1} \cdots x_{j_m}) = x_{i_1} \cdots x_{i_n} x_{j_1} \cdots x_{j_m}.$$

É de fácil verificação que $F\langle X\rangle$, munida dessa multiplicação, é uma álgebra associativa unitária.

Os elementos de X são chamados de **variáveis**, os elementos da forma $\alpha x_{i_1} \cdots x_{i_n}$, com $\alpha \in F$ e $n = 0, 1, 2, \ldots$ são chamados de **monômios** e os elementos de $F\langle X\rangle$ são chamados de **polinômios**. Em alguns momentos do texto, chamaremos aos polinômios de $F\langle X\rangle$ de **polinômios ordinários**. Essa nomenclatura será usada para distinguir os polinômios ordinários dos polinômios graduados, que definiremos mais a frente.

Proposição 2.1.2. *Para qualquer conjunto X, a álgebra $F\langle X\rangle$ é livre na classe das álgebras associativas unitárias.*

Demonstração. Seja A uma álgebra associativa unitária e $f : X \to A$ uma função qualquer. Considere também um conjunto de índices I tal que $X = \{x_i \ : i \in I\}$. Denote por a_i a imagem de x_i por f para cada $i \in I$. Dado um polinômio $p \in F\langle X\rangle$, denotaremos $p = p(x_{i_1}, \ldots, x_{i_s})$ se na expressão de p não aparecem os elementos x_i com $i \in A - \{i_1, \ldots, i_s\}$. Então defina $\overline{f} : F\langle X\rangle \to A$ por

$$\overline{f}(p(x_{i_1}, \ldots, x_{i_s})) = p(a_{i_1}, \ldots, a_{i_s})$$

(Aqui entende-se $p(a_{i_1}, \ldots, a_{i_s})$ a substituição de x_{i_j} por a_{i_j} na expressão de p, interpretando a concatenação de a's com sendo o produto em A.) Temos que $\overline{f}$ é um homomorfismo de álgebras tal que $\overline{f}|_X = f$. □

Exemplo 2.1.3. *Para qualquer conjunto X, a álgebra comutativa livre unitária $F[X]$ é livre na classe das álgebras associativas comutativas, livremente gerada por X. Para demonstrar esse fato, usamos um argumento similar ao usado na proposição anterior.*

Exemplo 2.1.4 (Comutador de Lie)**.** *Denotamos o polinômio* $(x_1x_2 - x_2x_1) \in F\langle X\rangle$ *por* $[x_1, x_2]$ *e o chamamos de* ***comutador de*** x_1, x_2 ***de comprimento*** 2*. Podemos definir indutivamente o comutador de comprimento* n *por*

$$[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n].$$

Observamos que o comutador é multilinear, no sentido de que

$$[x_1, \ldots, x_{i-1}, x_i + x_i', x_{i+1}, \ldots, x_n] = [x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n] + [x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n].$$

2.1.1 Identidades polinomiais

A menos que seja mencionado o contrário, X denotará um conjunto infinito enumerável de variáveis, isto é,

$$X = \{x_1, x_2, \ldots\}$$

e $F\langle X\rangle$ a álgebra polinomial associativa livre, livremente gerada por X. Denotaremos um polinômio $f \in F\langle X\rangle$ por $f(x_1, \ldots, x_n)$ se nenhuma outra variável x_j, $j \neq 1, \ldots, n$, aparece na expressão de f.

Definição 2.1.5. *Seja* R *uma álgebra associativa e* $f(x_1, \ldots, x_n) \in F\langle X\rangle$*. Dizemos que* f *é uma* ***identidade polinomial*** *para* R *se* $f(r_1, \ldots, r_n) = 0$*, para quaisquer* $r_1, \ldots, r_n \in R$*. Denotaremos por* $T(R)$ *o conjunto das identidades polinomiais de* R*. Se* $T(R) \neq \{0\}$*, dizemos que* R *é uma* ***PI-álgebra****. Duas álgebras associativas* A *e* B *são ditas PI-equivalentes se* $T(A) = T(B)$*.*

Em alguns momentos do texto chamaremos as identidades polinomiais de **identidades ordinárias**, para fazer distinção do conceito de identidade graduada que definiremos mais a frente. Observamos que nem toda álgebra é uma PI-álgebra. A própria álgebra $F\langle X\rangle$ é um contraexemplo. A seguir, alguns exemplos de PI-álgebras:

Exemplo 2.1.6. *Uma álgebra associativa* A *é comutativa se, e somente se,* $[x_1, x_2] \in T(A)$*.*

Exemplo 2.1.7 (Polinômio Standard)**.** *Se* R *é uma álgebra de dimensão finita, então* R

é uma PI-álgebra. Fixado $n \in \mathbb{N}$, defina

$$st_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)} \cdots x_{\sigma(n)},$$

*onde $(-1)^\sigma$ é o sinal da permutação σ. Chamamos esse polinônio de **polinômio standard de grau n**. Não é difícil ver que st_n é n-multilinear e alternado, isto é,*

$$st_n(x_1, \ldots, \alpha x_i + x_i', \ldots, x_n) = \alpha st_n(x_1, \ldots, x_i, \ldots, x_n) + st_n(x_1, \ldots, x_i', \ldots, x_n),$$

para qualquer $\alpha \in F$, e se $x_{\sigma(1)} \ldots x_i \ldots x_j \ldots x_{\sigma(n)}$ aparece com coeficiente ± 1 em st_n, então $x_{\sigma(1)} \ldots x_j \ldots x_i \ldots x_{\sigma(n)}$ aparece com coeficiente ∓ 1. Assim, tomando $n > \dim R$, temos que $st_n \in T(R)$.

Exemplo 2.1.8. *Seja E a álgebra de Grassmann gerada por $e_1, e_2 \ldots$. Então $[x_1, x_2, x_3] \in T(E)$. De fato, observe que*

$$(e_{i_1} \cdots e_{i_n})(e_{j_1} \cdots e_{j_m}) = (-1)^{mn}(e_{j_1} \cdots e_{j_m})(e_{i_1} \cdots e_{i_n}).$$

Assim, os monômios de comprimento par pertencem ao centro da álgebra de Grassmann. Considere agora monômios $u, v, w \in E$. Se algum desses monômios, digamos u, tem comprimento par então $u \in Z(E)$. Daí $[u, v, w] = [[u, v], w] = [0, w] = 0$. Se todos têm comprimento ímpar, então

$$[u, v, w] = [uv - vu, w] = [2uv, w] = 0$$

pois $2uv$ terá comprimento par. Da multilinearidade do comutador, segue a afirmação.

Exemplo 2.1.9 (Polinômio de Hall)**.** *O polinômio de Hall*

$$[[x_1, x_2]^2, x_3]$$

é uma identidade polinomial para $M_2(F)$. Tal fato segue do teorema de Cayley-Hamilton (ver em [10]).

Definição 2.1.10. *Seja I um ideal de $F\langle X\rangle$. Dizemos que I é um **T-ideal** se $\varphi(I) \subset I$,* *para todo endomorfismo φ de $F\langle X\rangle$. Equivalentemente, I é um T-ideal se*

$$f(g_1, \ldots, g_n) \in I$$

para todos $f(x_1, \ldots, x_n) \in I$ e $g_1, \ldots, g_n \in F\langle X\rangle$.

Exemplo 2.1.11. *Seja R uma álgebra associativa. Então não é difícil ver que $T(R)$ é um T-ideal. Reciprocamente, se I é um T-ideal de $F\langle X\rangle$ então existe uma álgebra R tal que $T(R) = I$. De fato, basta ver que*

$$T\left(\frac{F\langle X\rangle}{I}\right) = I.$$

Definição 2.1.12. *Seja $\{f_i \ : i \in I\}$ um subconjunto de $F\langle X\rangle$. A classe $\mathfrak{V}$ de todas as álgebras associativas R tais que $f_i \in T(R)$, $\forall i \in I$, é chamada de* ***variedade de álgebras associativas determinada por*** *$\{f_i \ : i \in I\}$. Uma variadade $\mathfrak{V}'$ é chamada subvariedade de $\mathfrak{V}$ se $\mathfrak{V}' \subset \mathfrak{V}$. O conjunto de todas as identidades polinomiais satisfeitas por todas as álgebras da variedade $\mathfrak{V}$ é denotado por $T(\mathfrak{V})$ e chamado de* ***T-ideal de*** *$\mathfrak{V}$. Neste caso, dizemos que $T(\mathfrak{V})$ é* ***gerado como T-ideal*** *por $\{f_i \ : i \in I\}$. Usamos a notação $T(\mathfrak{V}) = \langle f_i \ : i \in I\rangle^T$ e dizemos que $\{f_i \ : i \in I\}$ é uma* ***base para as identidades polinomiais de*** *$\mathfrak{V}$. Os elementos de $T(\mathfrak{V})$ são chamados de* ***consequências*** *dos $f_i's$.*

Justifica-se a escolha do nome de $T(\mathfrak{V})$ pelo fato de que tal conjunto é uma interseção de T ideais, o que também é um T-ideal.

Exemplo 2.1.13. *A classe de todas as álgebras associativas comutativas é uma variedade definida pelo polinômio $[x_1, x_2]$.*

Dada uma classe $\mathfrak{V}$ de álgebras, o próximo resultado dá um critério de quando $\mathfrak{V}$ é uma variedade.

Teorema 2.1.14 (Birkhoff). *Uma classe $\mathfrak{V}$ de álgebras é uma variedade se, e somente se, $c(\mathfrak{V})$, $s(\mathfrak{V})$ e $q(\mathfrak{V})$ estão contidos em $\mathfrak{V}$, onde*

$c(\mathfrak{V})$ é a classe formada por todos os produtos cartesianos de álgebras de $\mathfrak{V}$;

$s(\mathfrak{V})$ é a classe de todas as subálgebras das algebras de $\mathfrak{V}$;

$q(\mathfrak{V})$ é a classe de todas as álgebras quocientes das álgebras de $\mathfrak{V}$.

Demonstração. [10] Teorema 2.3.2, p. 24. □

Definição 2.1.15. *Dizemos que uma variedade $\mathfrak{V}$ tem* ***base finita para suas identidades polinomiais*** *se existe $S \subset F\langle X\rangle$ finito tal que S determina $\mathfrak{V}$.*

Naturalmente vem a pergunta: Toda variedade tem base finita para suas identidades polinomiais? Esse é o famoso problema de Specht. Em 1987, Kemer [18] provou que se $char\ F = 0$ então a resposta ao problema era afirmativa. Em 1999, Belov [5],[6], Grishin [14] e Shchigolev [25] mostraram que se $char\ F = p \neq 0$ então a resposta à pergunta é negativa. Um outro obstáculo nessa mesma linha é encontrar uma base para as identidades polinomiais de uma PI-álgebra. Drensky [11] mostrou em 1981 que os polinômios $st_4(x_1, x_2, x_3, x_4)$ e $[[x_1, x_2]^2, x_1]$ formam uma base para as identidades polinomiais de $M_2(F)$, com F de característica 0. O polinômio de Hall em duas variáveis $[[x_1, x_2]^2, x_1]$ é consequência do polinômio

$$p_{n+1}(x, y_1, \dots, y_n) = \sum_{\sigma\in S_{n+1}} x^{\sigma(0)}y_1x^{\sigma(1)}y_2\cdots y_nx^{\sigma(n)}$$

com $n = 2$, onde S_{n+1} age em $\{0, 1, \dots, n\}$. Havia esperança de que st_{2n} e p_{n+1} formassem uma base para $T(M_n(F))$ com $n > 2$. Porém, Okhitin [22] em 1986 e Domokos [9] em 1995 construíram identidades polinomiais para $M_3(F)$ que não eram consequências de st_6 e p_4. O problema de se encontrar explicitamente uma base para $M_n(F)$ para $n \geq 3$ permanece em aberto no caso geral.

Exemplo 2.1.16. *Se F é infinito então $T(U_n(F)) = \langle[x_1, x_2][x_3, x_4]\cdots[x_{2n-1}, x_{2n}]\rangle^T$.*

Exemplo 2.1.17. *Se F é infinito e R uma F-álgebra comutativa unitária. Então $T(F) = \langle[x_1, x_2]\rangle^T$ e $T(R) = \langle[x_1, x_2]\rangle$.*

O exemplo anterior mostra que o fato de duas álgebras terem as mesmas identidades polinomiais não implica que as duas álgebras são isomorfas. Tome como contraexemplo as $\mathbb{Q}$-álgebras $\mathbb{R}$ e $\mathbb{Q}$. Temos $T(\mathbb{R}) = \langle[x_1, x_2]\rangle = T(\mathbb{Q})$, porém $\mathbb{R}$ não é isomorfa a $\mathbb{Q}$.

2.2 Álgebras graduadas

Comecemos a seção fixando algumas notações. Seja R uma álgebra associativa sobre um corpo F e G um grupo com identidade e. R é dita ser uma **álgebra G-graduada** (ou simplesmente **álgebra graduada**, se o grupo estiver claro no contexto) se existe uma decomposição em espaços vetoriais

$$R = \bigoplus_{g \in G} R_g$$

tal que os subespaços R_g satisfazem a condição $R_g R_h \subset R_{gh}$, para todos $g, h \in G$. Cada subespaço R_g recebe o nome de **componente homogênea** da graduação. Em particular, a componente R_e é chamada de **componente identidade**. Para cada $g \in G$, um elemento $r \in R_g$ é chamado de **homogêneo de grau** g e denotamos $deg(r) = g$.

Um subespaço $V \subset R$ é dito ser um **subespaço graduado** (ou **subespaço homogêneo**) se

$$V = \bigoplus_{g \in G} (V \cap R_g).$$

Uma subálgebra A de R é dita ser uma **subálgebra graduada** se A é um subespaço graduado. Um ideal I(à esquerda, à direita ou bilateral) de R é dito ser um **ideal graduado** se I for um subespaço graduado de R.

Exemplo 2.2.1. *Considere a álgebra de Grassmann E com base $\{e_1, e_2, \ldots\}$ definida no exemplo 1.1.7. Ela tem uma $\mathbb{Z}_2$-graduação natural, onde E_0 é o subespaço de E gerado por $\{e_{i_1} e_{i_2} \cdots e_{i_k} \ : k \text{ é par}\}$ e E_1 é o subespaço de E gerado por $\{e_{i_1} e_{i_2} \cdots e_{i_m} \ : m \text{ é ímpar}\}$.*

Definição 2.2.2. *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra G-graduada. Dizemos que R é uma **álgebra G graduada simples** se $R^2 \neq 0$ e se R não possui ideais bilaterais graduados não triviais. R é dita ser uma **álgebra G-graduada de divisão** se R é unitária e todo elemento homogêneo não nulo de R for invertível.*

O seguinte resultado, que omitiremos a demonstração, é frequentemente usado para se decidir se um dado ideal de uma álgebra graduada é também graduado.

Lema 2.2.3. *Seja R uma álgebra G-graduada e I um ideal de R. Então I é um ideal graduado de R se, e somente se, I é gerado(como ideal) por elementos homogêneos.*

Sejam $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G} B_g$ duas álgebras G-graduadas. Um homomorfismo (isomorfismo) de álgebras $f : A \to B$ é dito ser um **homomorfismo de álgebras graduadas** se $f(A_g) \subset B_g$, para todo $g \in G$. Se existe um isomorfismo de álgebras graduadas entre duas álgebras graduadas A e B, então dizemos que A e B são **G-isomorfas**.

Dados, arbitrariamente, uma álgebra R e um grupo G, sempre podemos definir uma G-graduação em R pondo $R_g = 0$, para todo $g \neq e$ e $R_e = R$. Essa graduação é chamada de **graduação trivial**.

Definição 2.2.4. *Seja $R = \sum_{g\in G} R_g$ uma álgebra G-graduada. Definimos o* ***suporte*** *de R como sendo o conjunto*

$$supp(R) = \{g \in G \ : R_g \neq 0\}.$$

Cabe observar que o suporte não necessariamente é um subgrupo de G. De fato, se $R^2 = 0$, então $supp(R)$ pode ser um subconjunto arbitrário de G. Vejamos agora alguns exemplos de graduações importantes:

Exemplo 2.2.5 (Graduações elementares)**.** *Sejam $R = M_n(F)$ a álgebra das matrizes $n \times n$ sobre F e G um grupo. Fixe uma n-upla $u = (g_1, \ldots, g_n) \in G^n$. Denotando por E_{ij} as matrizes elementares de R, $1 \leq i, j \leq n$, podemos definir a seguinte graduação em R: para cada $g \in G$, defina*

$$R_g = Span\{E_{ij} \ : g_i^{-1}g_j = g\}.$$

Primeiro observe que

$$R = \bigoplus_{g\in G} R_g.$$

Além disso, se $E_{ij} \in R_g$ e $E_{kl} \in R_h$, temos que se $j \neq k$ então $E_{ij}E_{kl} = 0 \in R_{gh}$. Se $j = k$ então $E_{ij}E_{jl} = E_{il}$ e $g_i^{-1}g_l = g_i^{-1}g_jg_j^{-1}g_l = gh$, isto é, $E_{il} \in R_{gh}$. Portanto, a decomposição definida é de fato uma graduação. Essa graduação recebe o nome de ***graduação elementar****.*

O seguinte lema técnico será útil mais adiante:

Lema 2.2.6. *Considere a álgebra $R = M_n(F)$ munida de uma G-graduação $R = \bigoplus_{g\in G} R_g$. Se as matrizes escalares estão na componente unitária R_e e todas as matrizes E_{ii}, $i =$*

$1, \dots, n$ são homogêneas então a graduação é elementar.

Demonstração. Ver em [26] (p. 29). □

Se $a \in G$ é fixado, então a n-upla $(ag_1, \dots, ag_n)$ define a mesma estrutura de graduação uma vez que $(ag_i)^{-1}(ag_j) = g_i^{-1}g_j$. Assim, podemos sempre assumir que $g_1 = e$.

Lema 2.2.7. *Sejam $R = M_n(F)$, $\sigma \in S_n$ e fixe elementos $g_1, \dots, g_n \in G$. Considere as duas n-uplas $u = (g_1, \dots, g_n)$ e $v = (g_{\sigma(1)}, \dots, g_{\sigma(n)})$. Denote por R^u e R^v as estruturas de graduação definidas por u e v em R, respectivamente. Então R^u e R^v são álgebras G-graduadas isomorfas.*

Demonstração. Denote $v = (h_1, \dots, h_n)$. Temos as estruturas $R^u = \bigoplus_{g\in G} R^u_g$ e $R^v = \bigoplus_{g\in G} R^v_g$, onde

$$R^u_g = Span\{E_{ij} \ : g_i^{-1}g_j = g\} \qquad R^v_g = \{E_{ij} \ : h_i^{-1}h_j = g\}$$

Defina $\alpha : R^u \to R^v$ por $\alpha(E_{ij}) = E_{kl}$, onde $\sigma(k) = i$ e $\sigma(l) = j$. É claro que α é um homomorfismo de álgebras. Além disso, se $E_{ij} \in R^u_g$ então $g_i^{-1}g_j = g$. Logo

$$deg(\alpha(E_{ij})) = deg(E_{kl}) = h_k^{-1}h_l = g_{\sigma(k)}^{-1}g_{\sigma(l)} = g_i^{-1}g_j = g = deg(E_{ij})$$

o que mostra que α é um isomorfismo de álgebras G-graduadas. □

Exemplo 2.2.8 (Produto tensorial de álgebras)**.** *Sejam G e H dois grupos e $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{h\in H} B_h$ álgebras G-graduada e H-graduada, respectivamente. Então o produto tensorial $C = A \otimes B$ é $(G\times H)$-graduado de modo natural. Definimos, para cada $(g, h) \in G \times H$,*

$$C_{(g,h)} = A_g \otimes B_h.$$

Não é difícil ver que as componentes $C_{(g,h)}$ estão todas em soma direta e que

$$C = \bigoplus_{(g,h)\in G\times H} C_{(g,h)}.$$

Considere agora duas álgebras G-graduadas, $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G} B_g$ e denote $S = supp(A)$ e $T = supp(B)$. Se os elementos de S e T comutam aos pares, então o *produto tensorial* $C = A \otimes B$ *pode ser* G*-graduado pondo*

$$C_t = \bigoplus_{gh=t} (A_g \otimes B_h)$$

Mostremos primeiro que os subespaços C_t *estão em soma direta.*

Para cada $g, h \in G$*, sejam* $\{a_\lambda^g\}_{\lambda \in I_g}$ *base para* A_g *e* $\{b_\delta^h\}_{\delta \in J_h}$ *base para* B_h*. Então os conjuntos*

$$\bigcup_{g \in G} \{a_\lambda^g\}_{\lambda \in I_g} \qquad \bigcup_{h \in G} \{b_\delta^h\}_{\delta \in J_h}$$

são bases para A *e* B *respectivamente. Então o conjunto*

$$\bigcup_{(g,h) \in G \times G} \{a_\lambda^g \otimes b_\delta^h\}_{\lambda \in I_g,\ \delta \in J_h} \tag{2.2.1}$$

é base para C*. Para cada* $t \in G$*, considere todos* $g, h \in G$ *tais que* $gh = t$*. Então*

$$\Gamma_t = \bigcup_{gh=t} \{a_\lambda^g \otimes b_\delta^h\}_{\lambda \in I_g,\ \delta \in J_h}$$

é base para C_t*. Observe então que* $\Gamma_t \cap \Gamma_s = \emptyset$ *se* $t \neq s$*, uma vez que (2.2.1) é base para* C*. Portanto os subespaços* C_t *estão em soma direta e* $C = \bigoplus_{t \in G} C_t$*. Usando que os elementos de* S *e* T *comutam aos pares, não é difícil ver que* $C_t C_s \subset C_{ts}$*.*

No segundo momento do exemplo anterior, temos que se duas álgebras A e B são G-graduadas e $S = supp(A)$ e $T = supp(B)$ comutam aos pares então podemos definir uma G-graduação no produto tensorial $C = A \otimes B$ pondo $C_t = \bigoplus_{gh=t} A_g \otimes B_h$ para cada $t \in G$. Essa definição de graduação no produto tensorial é possível, em particular, se G é abeliano. Para o caso não abeliano, não é possível, em geral, estender essa definição. Porém, no caso especial a seguir, apresentamos uma extensão desse conceito.

Exemplo 2.2.9 (Graduações induzidas no produto tensorial)**.** *Sejam* $A = M_n(F)$ *uma álgebra de matrizes com uma* G*-graduação elementar definida por uma* n*-upla* $(g_1, \ldots, g_n)$ *e* $B = \bigoplus_{g \in G} B_g$ *uma álgebra* G*-graduada qualquer. Então pode-se induzir uma* G*-*

graduação no produto tensorial $C = A \otimes B$ *definindo para cada* $g \in G$

$$C_g = Span\{E_{ij} \otimes b \ : deg(b) = h, g_i^{-1}hg_j = g\}.$$

Então a decomposição $C = \bigoplus_{g \in G} C_g$ *é uma* G*-graduação e* B *é uma subálgebra* G*-graduada de* C*. Além disso, se* B *é unitária, então* A *é uma subálgebra graduada de* C*. Essa graduação recebe o nome de* ***graduação induzida no produto tensorial****.*

Exemplo 2.2.10 (Álgebra de grupo twisted)**.** *Sejam* F *um corpo e* G *um grupo. Considere a álgebra de grupo* $F[G]$ *consistindo no* F*-espaço vetorial com base* $\{r_g \ : g \in G\}$ *com multiplicação dada por* $r_g r_h = r_{gh}$*, para quaisquer* $g, h \in G$*. Então* $F[G]$ *pode ser equipada com uma graduação definindo para cada* $g \in G$*,*

$$R_g = Span\{r_g\}.$$

Essa graduação recebe o nome de ***graduação canônica****. Observe que* $F[G]$ *com a graduação canônica é uma álgebra graduada de divisão pois todo elemento homogêneo não nulo é invertível.*

Considere agora uma aplicação $\sigma : G \times G \to F^*$ *e* $F^\sigma[G]$ *o espaço vetorial com base* $\{r_g \ : g \in G\}$ *e com produto*

$$r_g r_h = \sigma(g, h) r_{gh} \tag{2.2.2}$$

para quaisquer $g, h \in G$*. Para que este produto em* $F^\sigma[G]$ *seja associativo,* σ *deve satisfazer a relação*

$$\sigma(x, y)\sigma(xy, z) = \sigma(y, z)\sigma(x, yz) \tag{2.2.3}$$

para quaisquer $x, y, z \in G$*. Uma aplicação* $\sigma : G \times G \to F^*$ *satisfazendo* (2.2.3) *é chamada de* 2-cociclo em G com valores em F *e a álgebra associativa* $F^\sigma[G]$ *com produto* (2.2.2) *recebe o nome de* ***álgebra de grupo twisted****. Se definirmos*

$$(F^\sigma[G])_g = Span\{r_g\}$$

então $F^{\sigma}[G]$ se torna uma álgebra G-graduada e dizemos que tal graduação é canônica. *Obviamente, se $\sigma \equiv 1$ então $F^{\sigma}[G]$ se torna a álgebra de grupo ordinária.*

A álgebra de grupo twisted $F^{\sigma}[G]$ é uma álgebra de divisão graduada.

Para mais propriedades da álgebra de grupo twisted, indicamos [23] e [24]. Recordemos a definição de álgebra semissimples:

Definição 2.2.11. *Seja R uma álgebra de dimensão finita. Dizemos R é* ***semissimples*** *se R não possui ideais nilpotentes não nulos. Definimos o* ***Radical de Jacobson de*** *R como sendo a interseção de todos os ideais primitivos de R. Como R tem dimensão finita então o Radical de Jacobson de R é o único ideal maximal nilpotente de R.*

Proposição 2.2.12. *Seja G um grupo tal que $|G|$ é invertível no corpo F. Então $F^{\sigma}[G]$ é semissimples para qualquer 2-cociclo σ em G.*

Demonstração. Ver em [24] (teorema 4.4). □

2.3 Identidades graduadas

Como trabalharemos com identidades polinomiais em álgebras graduadas, precisamos do conceito de polinômio graduado. Dado um grupo G, seja $\{X_g : g \in G\}$ uma família de conjuntos infinitos enumeráveis disjuntos. Defina $X = \bigcup_{g \in G} X_g$ como um conjunto de variáveis. Então a álgebra associativa livre $F\langle X\rangle$ pode ser equipada com uma G graduação da seguinte maneira: defina $deg(x) = g$ para todo $x \in X_g$, $deg(1) = e$ e $deg(x_1 \cdots x_n) = deg(x_1) \cdots deg(x_n)$. Assim, fica definido o subespaço

$$F\langle X\rangle_g = Span\{u \ : u \text{ é monômio de } F\langle X\rangle \text{ e } deg(u) = g\}.$$

Assim, vale que

$$F\langle X\rangle = \bigoplus_{g \in G} F\langle X\rangle_g \quad \text{e} \quad F\langle X\rangle_g F\langle X\rangle_h \subset F\langle X\rangle_{gh}.$$

Usaremos a notação $x = x^g$ quando $x \in X_g$ e chamaremos a álgebra $F\langle X\rangle$ com a graduação acima de **álgebra associativa livre G-graduada**. Os elementos de $F\langle X\rangle$

são chamados de **polinômios graduados**. A álgebra G-graduada $F\langle X\rangle$ satisfaz a seguinte propriedade: para qualquer álgebra G-graduada $A = \bigoplus_{g\in G} A_g$, toda função $\varphi : X = \bigcup_{g\in G} X_g \to A$ tal que $\varphi(X_g) \subset A_g$, para todo $g \in G$, pode ser estendida a um único homomorfismo de álgebras $\Phi : F\langle X\rangle \to A$ tal que $\Phi|_X = \varphi$.

Vamos agora ao conceito de identidade polinomial graduada:

Definição 2.3.1. *Sejam G um grupo, $R = \bigoplus_{g\in G} R_g$ uma álgebra graduada e $f = f(x_1^{g_1}, \ldots, x_n^{g_n}) \in F\langle X\rangle$ um polinômio graduado. Dizemos que f é uma* ***identidade polinomial graduada para*** *R se $f(r_1, \ldots, r_n) = 0$ para quaisquer $r_1 \in R_{g_1}, \ldots, r_n \in R_{g_n}$. Denotaremos por $T_G(R)$ o conjunto das identidades polinomiais G-graduadas de R.*

Temos a noção análoga de T-ideal para o caso de polinômios graduados:

Definição 2.3.2. *Sejam G um grupo e $F\langle X\rangle$ a álgebra associativa livre G-graduada. Um ideal I de $F\langle X\rangle$ é dito ser um* ***T_G-ideal*** *se $\varphi(I) \subset I$ para todo endomorfismo G-graduado φ de $F\langle X\rangle$.*

Assim, como no caso das identidades ordinárias, temos o seguinte resultado:

Lema 2.3.3. *Se $R = \bigoplus_{g\in G} R_g$ for uma álgebra G-graduada então o conjunto das identidades graduadas de R, $T_G(R)$, é um T_G-ideal de $F\langle X\rangle$.*

Podemos relacionar os conceitos de identidades graduadas e identidades ordinárias. Esse resultado tem conexão direta com o resultado principal deste trabalho.

Proposição 2.3.4. *Sejam G um grupo e $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G} B_g$ duas álgebras G-graduadas. Se $T_G(A) \subset T_G(B)$ então $T(A) \subset T(B)$. Em particular, se $T_G(A) = T_G(B)$ então $T(A) = T(B)$.*

Demonstração. Por conta da notação, considere a álgebra associativa livre $F\langle Y\rangle$, onde $Y = \{y_1, y_2, \ldots, y_n, \ldots\}$. Seja $f = f(y_1, \ldots, y_n) \in T(A)$. Dados arbitrariamente $b_1, \ldots, b_n \in B$, escreva

$$b_i = b^i_{g_{i1}} + b^i_{g_{i2}} + \cdots + b^i_{g_{im_i}},$$

onde $b^i_{g_{ij}} \in B_{g_{ij}}$, $j = 1, \ldots, m_i$. Considere agora o polinômio graduado

$$\widetilde{f} = f\left(\sum_{j=1}^{m_1} x_1^{g_{1j}}, \ldots, \sum_{j=1}^{m_n} x_n^{g_{nj}}\right).$$

Como $f \in T(A)$, note que $\widetilde{f} \in T_G(A)$, o que implica por hipótese que $\widetilde{f} \in T_G(B)$. Assim,

$$f(b_1, b_2, \ldots, b_n) = f\left(\sum_{j=1}^{m_1} b^1_{g_{1j}}, \sum_{j=1}^{m_2} b^2_{g_{2j}}, \ldots, \sum_{j=1}^{m_n} b^n_{g_{nj}}\right) = \widetilde{f}(b^1_{g_{11}}, \ldots, b^n_{g_{nm_n}}) = 0,$$

isto é, $f \in T(B)$. Logo, se $T_G(A) = T_G(B)$ então $T_G(A) \subset T_G(B)$ implica $T(A) \subset T(B)$ e $T_G(B) \subset T_G(A)$ implica $T(B) \subset T(A)$, como queríamos. $\square$

A proposição anterior mostra que se duas álgebras G graduadas possuem as mesmas identidades graduadas então elas possuem as mesmas identidades ordinárias, isto é, são PI-equivalentes. Porém se duas álgebras graduadas satifazem as mesmas identidades ordinárias, não se pode dizer que satisfazem as mesmas identidades graduadas.

Exemplo 2.3.5. *Considere a álgebra de Grassmann $E = E_0 \oplus E_1$ com a $\mathbb{Z}_2$-graduação. Considere novamente a álgebra de Grassmann com a graduação trivial por $\mathbb{Z}_2$. Então $E = E_0 \oplus E_1$ e $E = E \oplus 0$ satisfazem obviamente as mesmas identidades mas não satisfazem as mesmas identidades graduadas pois o polinômio graduado $f(x_1^1) = x_1^1$ é identidade graduada para E com a graduação trivial, porém não é para E com a $\mathbb{Z}_2$-graduação canônica.*

Capítulo 3

Álgebras graduadas simples de dimensão finita

O objetivo deste capítulo é descrever as álgebras graduadas simples, impondo certas condições ao corpo sobre o qual a álgebra está construída e sobre sua dimensão. Nesta seção, G será um grupo qualquer e um idempotente que é também homogêneo será chamado de *idempotente graduado*.

3.1 Unitariedade de álgebras graduadas simples

Nesta seção mostraremos que se F é um corpo qualquer então uma F-álgebra graduada simples de dimensão finita R é unitária.

Lema 3.1.1. *Sejam $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada simples de dimensão finita e $I \subset R$ um ideal minimal à direita graduado de R. Então $I = aR$, para algum idempotente graduado a.*

Demonstração. Suponha que $I^2 = 0$. Então $(RI)^2 = R(IR)I \subset RI^2 = 0$ o que implica que o ideal bilateral RI de R é nilpotente. Observe que RI é um ideal graduado de R. Logo $RI = R$ ou $RI = 0$. O primeiro caso não pode ocorrer pois $R^2 \neq 0$. Logo $RI = 0$. Assim I é um ideal bilateral não trivial graduado de R, uma contradição. Logo devemos ter $I^2 \neq 0$ e então existe elemento homogêneo não nulo x em I tal que $xI \neq 0$. Da minimalidade de I, segue que $xI = I$. Em particular, $xa = x$, para algum $a \in I$. Defina o anulador à direita de x em R, isto é, o conjunto

$$Ann_R(x) = \{r \in R \ : xr = 0\}.$$

Observe que $Ann_R(x)$ é um ideal à direita graduado de R (pois x é homogêneo). Além disso, devemos ter $Ann_R(x) \cap I = 0$ ou $Ann_R(x) \cap I = I$, pois caso contrário teríamos uma contradição com a minimalidade de I. O segundo caso não pode ocorrer pois $a \in I$ mas $a \notin Ann_R(x)$. Logo devemos ter $Ann_R(x) \cap I = 0$. Assim, como $xa^2 = xa$, isto é $x(a^2 - a) = 0$. Consequentemente, a é idempotente graduado. Portanto, como aI é um ideal à direita não nulo (pois $a^2 = a \neq 0$), segue que $aI = I$. $\square$

Lema 3.1.2. *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra G-graduada simples de dimensão finita e $I \subset R$ um ideal à direita não nulo. Então $I = bR$ para algum idempotente graduado b.*

Demonstração. Como a dimensão de R é finita, I contém algum ideal minimal à direita não nulo. Pelo lema anterior, I contém um idempotente graduado a. Para cada idempotente graduado $t \in I$, defina o anulador à direita de t em I, isto é, o conjunto

$$Ann_I(t) := \{x \in I \ : tx = 0\}.$$

Afirmamos que existe um idempotente graduado b tal que $Ann_I(b) = 0$. Para isso, uma vez que R tem dimensão finita, é suficiente provarmos que se $Ann_I(a) \neq 0$ então é possível encontrar outro idempotente graduado $t \in I$ tal que $dim(Ann_I(t)) < dim(Ann_I(a))$.

Como a é homogêneo, o anulador de a em R, $Ann_R(a)$, é um ideal à direita graduado. Logo $Ann_I(a) = Ann_R(a) \cap I$ é também ideal à direita graduado de R. Como na demonstração anterior, existe um idempotente graduado não nulo $f \in Ann_I(a)$. Como $f^2 = f$ e $af = 0$, definimos o elemento

$$t := a + f - fa.$$

Então não é difícil ver que t é idempotente. Como a, t são idempotentes graduados então $a, t \in R_e$. Logo t também é idempotente graduado. Mostremos agora que $Ann_I(t)$ é subespaço próprio de $Ann_I(a)$. Tome $x \in Ann_I(t)$. Neste caso,

$$0 = tx = atx = a(a + f - fa)x = a^2x = ax,$$

isto é, $x \in Ann_I(a)$. Entretanto,

$$tf = (a + f - fa)f = f^2 = f \neq 0.$$

Portanto $Ann_I(t) \neq Ann_I(a)$. Como a dimensão é finita, continuamos o processo até encontrar um idempotente graduado não nulo $b \in I$ tal que $Ann_I(b) = 0$. Como para qualquer $x \in I$ tem-se $b(x - bx) = 0$, segue que $x = bx$,o que implica que $bI = I$, como queríamos demonstrar. □

Já estamos prontos para demonstrar o principal resultado desta seção:

Teorema 3.1.3. *Seja R uma álgebra graduada simples de dimensão finita sobre um corpo arbitrário F. Então R é unitária.*

Demonstração. Pelo lema anterior, existe idempotente graduado $a \in R$ tal que $aR = R$ (basta tomar $I = R$ no lema anterior). Ainda pela demonstração do teorema anterior, podemos tomar tal elemento de modo que $Ann_R(a) = 0$. Para qualquer $x \in R$, tem-se que $a(ax - x) = 0$, isto é, $ax = x$. Defina

$$I = \{x - xa \ : x \in R\}.$$

Observe que I é um ideal à esquerda graduado. De fato, se $x = r_{g_1} + \cdots + r_{g_n} \in R$ com $r_{g_i} \in R_{g_i}$, temos

$$x - xa = r_{g_1} - r_{g_1}a + \cdots + r_{g_n} - r_{g_n}a \in \bigoplus_{g \in G} I \cap R_g$$

pois $a \in R_e$. Além disso, $Ia = 0$. Portanto, $IR = IaR = 0$, e então I é um ideal bilateral graduado de R. Se $I = R$ então $R^2 = IR = 0$, o que é um absurdo. Logo devemos ter $I = 0$. Portanto, $ax = x = xa$ para qualquer $x \in R$. □

3.2 Álgebras graduadas de divisão

Nesta seção vamos descrever as álgebras de divisão graduadas de dimensão finita sobre um corpo F algebricamente fechado.

Lema 3.2.1. *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada de divisão de dimensão finita sobre um corpo algebricamente fechado F. Então $H = supp(R)$ é um subgrupo de G e $dim(R_h) = 1$ para todo $h \in H$.*

Demonstração. Se $g, h \in H$, então $R_g \neq 0$ e $R_h \neq 0$. Tome $0 \neq x \in R_g$ e $0 \neq y \in R_h$. Então $0 \neq xy \in R_{gh}$, isto é, $gh \in H$. Do mesmo modo, como x é invertível, segue que $0 \neq x^{-1} \in R_{g^{-1}}$, isto é, $g^{-1} \in H$. Portanto H é subgrupo de G.

Note que R_e é uma álgebra de divisão sobre o corpo F, que é algebricamente fechado. Pela proposição (1.1.13) temos que $R_e \cong F$. Portanto $dim(R_e) = 1$. Suponha agora que $g \neq e$ e seja $0 \neq x \in R_g$. Então x é invertível e $x^{-1} \in R_{g^{-1}}$. Tome $y \in R_g$ arbitrário. Então $yx^{-1} \in R_e$. Sendo R unitária, segue que $1 \in R_e$. De fato, se $1 = x_e + \sum_{g\neq e} x_g$, com $x_g \in R_g$, então para $y \in R_h$ arbitrário, com $h \in G$, $y = yx_e + \sum_{g\neq e} yx_g$, ou seja, $y - yx_e = \sum_{g\neq e} yx_g$. Daí, devemos ter $h = deg(y - yx_e) = deg(\sum_{g\neq e} yx_g)$. Porém para todo $g \neq e$, $deg(yx_g) = deg(y)deg(x_g) = hg \neq h$. Mas então devemos ter $yx_g = 0$ para todo $g \neq e$ e então $y = yx_e \in R_e$. Do mesmo modo mostra-se que $y = x_e y$. Assim, a componente x_e comuta com todos os elementos homogêneos de R. Logo $1 = x_e \in R_e$. Assim, existe $\alpha \in F$ tal que $yx^{-1} = \alpha 1$, o que implica que $y = \alpha x$. Como y foi arbitrário, segue que $dim(R_g) = 1$. □

Teorema 3.2.2. *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada de dimensão finita sobre um corpo algebricamente fechado F. Então R é uma álgebra G-graduada de divisão se, e somente se, R é G-isomorfa a uma álgebra de grupo twisted $F^\sigma[H]$ com H-graduação canônica, onde H é um subgrupo finito de G e $\sigma : H \times H \to F^*$ é um 2-cociclo em H.*

Demonstração. Já vimos que toda álgebra de grupo twisted é uma álgebra de divisão graduada com a graduação canônica. Provemos a recíproca. Defina $H = supp(R)$. Pelo lema anterior, H é subgrupo de G e é finito pois R tem dimensão finita. Como estamos assumindo que R é uma álgebra graduada de divisão, segue também pelo lema anterior que $dim(R_h) = 1$ para todo $h \in H$. Para cada $h \in H$, fixe elemento não nulo $x_h \in R_h$.

Escolhendo arbitrariamente $g, h \in H$, existe um escalar não nulo, que denotaremos por $\sigma(g,h) \in F^*$, tal que

$$x_g x_h = \sigma(g,h) x_{gh}.$$

Assim fica determinada uma função $\sigma : H \times H \to F^*$. Como R é uma álgebra associativa, σ deve satisfazer

$$\sigma(g,h)\sigma(gh,t) = \sigma(h,t)\sigma(h,ht)$$

para quaisquer $g, h, t \in H$. Deste modo, σ é um 2-cociclo e a aplicação $\varphi : R \to F^\sigma[H]$ dada por $\varphi(x_h) = r_h$ é um isomorfismo de álgebras graduadas. □

Proposição 3.2.3. *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo arbitrário F. Se $dim(R_e) = 1$ então R é uma álgebra graduada de divisão.*

Demonstração. Como $dim(R_e) = 1$ segue que $R_e \cong F$ e portanto todo elemento não nulo de R_e é invertível. Tome $x \in R_g$, com $g \neq e$. O ideal bilateral RxR é graduado em R (pois x é homogêneo) e portanto $RxR = R$. Em particular existem homogêneos $a, b \in R$ tais que $0 \neq axb \in R_e$. Como $R_e \cong F$, podemos assumir sem perda de generalidade que $axb = 1$. Como $dim(R)$ é finita então R é Dedekind-finita, isto é,

$$1 = (ax)b = b(ax) = (ba)x = xba$$

o que mostra que $ba = x^{-1}$. □

3.3 Semissimplicidade de álgebras graduadas simples

Nesta seção provaremos que uma F-álgebra graduada simples R de dimensão finita, dadas certas condições sobre o corpo F, é semissimples, isto é, R não possui ideais nilpotentes não nulos (ou equivalentemente que R possui radical de Jacobson nulo). Nesse sentido, por conta da imposição da finitude da dimensão da álgebra R, por diversas vezes usaremos a caracterização de álgebras semissimples dada pelo teorema de Wedderburn-Artin que é a seguinte: seja R uma F-álgebra de dimensão finita semissimples. Então R é isomorfa a um produto direto finito de álgebras de matrizes sobre F-álgebras de divisão, isto é, R é da forma

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t),$$

para inteiros positivos $n_1, \ldots, n_t$ e álgebras de divisão $D_1, \ldots, D_t$. Observe que se F for algebricamente fechado, então pela proposição (1.1.13) segue que

$$R \cong M_{n_1}(F) \times \cdots M_{n_t}(F)$$

Para a demonstração do teorema de Wedderburn-Artin indicamos [7], [16] e [20].

Lema 3.3.1. *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo arbitrário F. Então R_e não possui ideais nilpotentes não nulos.*

Demonstração. Mostremos primeiramente o lema para ideais à esquerda. Seja I um ideal à esquerda nilpotente não nulo de R_e com, digamos, $I^m = 0$. Como R tem dimensão finita, então $supp(R)$ é finito. Denote $|supp(R)| = n$. Seja $J = RI$ o ideal à esquerda de R gerado por I. Mostremos que $J^{mn} = 0$. Para tal, basta mostrarmos que para arbitrários $x_1, \ldots, x_{mn} \in I$ e homogêneos não nulos $a_1, \ldots, a_{mn} \in R$ vale a igualdade

$$a_1x_1a_2x_2 \cdots a_{mn}x_{mn} = 0. \tag{3.3.1}$$

Como cada a_i é homogêneo não nulo, existem $g_1, \ldots, g_{mn} \in supp(R)$ tais que $a_i \in R_{g_i}, i = 1, \ldots, mn$. Defina os elementos:

$$u_1 = g_1,\ u_2 = g_1g_2,\ \ldots,\ u_{mn} = g_1g_2\cdots g_{mn}.$$

Se para algum $i = 1, \ldots, mn$ tivermos $u_i \notin supp(R)$ então $a_1x_1 \cdots a_ix_i \in R_{u_i} = 0$ e então a igualdade (3.3.1) vale. Se $u_i \in supp(R)$, para $i = 1, \ldots, mn$ e $|supp(R)| = n$ então pelo princípio da casa dos pombos, existem índices $i_1 < i_2 < \cdots < i_m$ tais que $u_{i_1} = \cdots = u_{i_m}$. Defina

$$b_k = a_{i_k+1}x_{i_k+1}a_{i_k+2}\cdots a_{i_{k+1}},\ k = 1, \ldots, m-1.$$

Observe que como $u_{i_k} = u_{i_{k+1}}$ segue que $g_{i_k+1}\cdots g_{i_{k+1}} = e$. Portanto, $deg(b_k) = e$, isto é

$b_1, \ldots, b_{m-1} \in R_e$. Observe que do lado esquerdo da igualdade (3.3.1) aparece o fator

$$c := x_{i_1} b_1 x_{i_2} b_2 \cdots x_{i_{m-1}} b_{m-1} x_{i_m}.$$

Como I é ideal à esquerda de R_e, segue que $c \in I^m = 0$. Portanto a igualdade 3.3.1 é verdadeira. Para ideais à direita, o argumento é análogo. Deste modo, o ideal RIR de R é nilpotente. Note que RIR é ideal graduado (pois é gerado por elementos homogêneos, uma vez que $I \subset R_e$) de R. Como $RIR = R$ não pode ocorrer (pois como R é unitária, $R^2 \subset R^s$ para todo $s \geq 2$. Daí teríamos $R^2 = 0$) devemos ter $RIR = 0$ o que implica que $I = 0$ □

Isso prova o seguinte resultado, referente à componente homogênea de uma álgebra graduada:

Corolário 3.3.2. *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo arbitrário F. Então R_e é semissimples.*

Lema 3.3.3. *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo arbitrário F e $t \in R_e$ um idempotente graduado. Então a subálgebra tRt é graduada simples.*

Demonstração. Denote $A := tRt$. Pelo teorema (3.1.3) R é unitária. Se $t = 1$ não há o que fazer. Suponha $t \neq 1$. Observe que como $t \in R_e$, a subálgebra A é graduada. Como $t \in A$, segue que $A^2 \neq 0$. Seja $I \subset A$ um ideal graduado de A com $I \neq A$. Considere o ideal $T = RIR$ de R gerado por I. Afirmamos que T é ideal graduado de R. De fato, dado $ras \in T$ com $a \in I$ e $r, s \in R$, escrevemos

$$r = \textstyle\sum_i r_{g_i},\, s = \sum_j s_{h_j},\, a = \sum_k a_{p_k} \text{ com } r_{g_i} \in R_{g_i},\, s_{h_j} \in R_{h_j} \text{ e}$$
$$a_{p_k} \in I_{p_k} = I \cap A_{p_k} = I \cap A \cap R_{p_k}.$$

Daí, temos que

$$ras = \sum_{i,j,k} r_{g_i} a_{p_k} s_{h_j} \in \bigoplus_{g \in G} RIR \cap R_g$$

e portanto T é graduada. Observe também que para todo $b \in I$ vale que $tbt = b$, uma vez que $I \subset A$. Agora afirmamos que $T \cap A = I$. Com efeito, se $y \in T \cap A$ então podemos escrever

$$y = \sum_i r_i x_i s_i, \text{ com } r_i, s_i \in R \text{ e } x_i \in I.$$

Assim,

$$y = tyt = \sum_i t r_i x_i s_i t = \sum_i (t r_i t) x_i (t s_i t) \in I.$$

A inclusão contrária é imediata e então $T \cap A = I$. Como R é graduada simples, devemos ter $T = R$ ou $T = 0$. Se $T = R$ então $I = T \cap A = R \cap A = A$, o que é uma contradição. Deste modo devemos ter $T = 0$ e, portanto, $I = 0$. □

Lema 3.3.4. *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo algebricamente fechado F, tal que $A = R_e$ é uma álgebra simples. Denote por C o centralizador de A em R. Então $R = AC \cong A \otimes C$, onde $A \cong M_k(F)$ e C é uma álgebra graduada de divisão.*

Demonstração. Observe primeiramente que C é subálgebra graduada. Com efeito, seja $c = c_1 + \cdots + c_n \in C$ com $c_i \in R_{g_i}$, para certos $g_i \in G$. Então para qualquer $a \in A$, devemos ter $ca = ac$, isto é,

$$\sum_i^n c_i a = \sum_i^n a c_i.$$

Como $deg(ac_i) = g_i = deg(c_i a)$, para $i = 1, \ldots, n$ segue que $c_i a = a c_i$ para $i = 1, \ldots, n$. Portanto $c \in \sum_{g \in G} C \cap R_g$, como queríamos. Para mostrar que C é uma álgebra de divisão graduada, observe que $C_e = C \cap R_e \subset R_e = A$. Daí, $dim(C_e) \leq dim(A \cap C) = dim(Z(A)) = 1$. Pela proposição (3.2.3) segue o desejado.

Pelo teorema de Wedderburn para álgebras segue que A é isomorfo a $M_k(D)$ para algum natural k e D é uma álgebra de divisão sobre F. Como D tem dimensão finita e F é algebricamente fechado então pela proposição (1.1.13) segue que $D \cong F$. Daí temos que $A \cong M_k(F)$. Deste modo, A possui uma base $\{u_{ij} \ : 1 \leq i, j \leq k\}$ tal que $u_{ij} u_{kl} = \delta_{jk} u_{il}$ e $1 = u_{11} + \cdots + u_{kk}$. Para cada $x \in R$, defina para fixados i, j o elemento

$$x_{ij} = \sum_s u_{si} x u_{js}.$$

Observe que $x_{ij} \in C$ pois para índices k, l arbitrários temos

$$x_{ij} u_{kl} = \sum_s u_{si} x u_{js} u_{kl} = u_{ki} x u_{jl} = u_{kl} x_{ij}$$

Logo $x_{ij} \in C$. Deste modo, tem-se que

$$AC \ni \sum_{i,j=1}^{k} u_{ij}x_{ij} = x$$

Portanto $R = AC$ e devemos ter $R \cong M_k(C) \cong A \otimes C$. $\square$

Teorema 3.3.5. *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada simples de dimensão finita sobre um corpo algebricamente fechado F tal que $char(F) = 0$ ou $char(F)$ é coprimo com a ordem de cada subgrupo finito de G. Então R é semissimples.*

Demonstração. Pelo corolário (3.3.2) R_e é semissimples. Assim, escreva $R_e \cong A^{(1)} \oplus \cdots \oplus A^{(m)}$, onde cada $A^{(i)}$ é uma álgebra de matrizes. Denote por e_i a identidade de $A^{(i)}$, para cada $i = 1, \ldots, m$. Pelo teorema (3.1.3) R é unitária e então $1 = e_1 + \cdots + e_m$. Observe que $e_1, \ldots, e_m$ é um sistema ortogonal de idempotentes e

$$R = \bigoplus_{1\le i,j\le m} e_iRe_j.$$

Fixe índice $1 \le i \le m$ e considere a subálgebra $B = e_iRe_i$. Pelo lema (3.3.3) temos que B é graduada simples e então pelo lema (3.3.4), $B \cong M_k(F) \otimes C \cong M_k(C)$, onde C é uma subálgebra de divisão graduada. Pelo teorema (3.2.2), temos que $C \cong F^\sigma[H]$, onde H é um subgrupo de G e $\sigma : H \times H \to F^*$ é um 2-cociclo. Como $char(F) = 0$ ou $char(F)$ é coprimo com a ordem de H, pela proposição (2.2.12), temos que $F^\sigma[H]$ é semissimples. Assim,

$$J(B) = J(M_k(F^\sigma[H])) \cong M_k(J(F^\sigma[H])) = 0.$$

Portanto B é semissimples.

Denote por $J = J(R)$ o radical de Jacobson de R. Pelo teorema 4.2 de [24], J é um ideal graduado de R. Note que vale

$$e_iJe_i = J \cap e_iRe_i = J(e_iRe_i) = 0.$$

Assuma que $J \neq 0$. Como $J = \bigoplus_{i,j} e_iJe_j$, temos que $e_kJe_l \neq 0$, para algum par de índices tal que $k \neq l$. Fixe $x \in e_kJe_l$ não nulo. Então, considere a decomposição $x = \sum_{g\in G} x_g$, com relação à G-graduação. Então,

$$x = e_k x e_l = \sum_g e_k x_g e_l. \tag{3.3.2}$$

Como $deg(e_k x_g e_l) = g = deg(x_g)$, temos que $x_g = e_k x_g e_l$. Daí, $x_g \in e_k R e_l \cap J$ pois $x_g \in J$ pois J é graduado em R. Assim, todas as componentes x_g pertencem a $e_k J e_l$. Em particular $e_i x_g e_j = 0$ se $i \neq k$ ou $j \neq l$.

Considere o conjunto $T = e_i R e_k x e_l R e_i$. Observe que $T \subset e_i R e_i \cap J$ (pois $x \in e_k J e_l \subset J$). Assim, $R e_k x e_l R \subset J$ (pois J é ideal), o que implica $T = 0$. Como toda componente x_g pertence a $e_k J e_l$, segue que $e_i R e_k x_g e_l R e_i = 0$ para toda componente homogênea x_g. Deste modo,

$$R x_g R = \bigoplus_{i,j,s,t} e_i R e_j x_g e_s R e_t = \bigoplus_{i \neq j} e_i R e_k x_g e_l R e_j. \tag{3.3.3}$$

Como $x_g = e_k x_g e_l$ e $x \neq 0$, usando a igualdade (3.3.2), tomemos uma componente x_g não nula. Observe então que o ideal $R x_g R$ é graduado em R. Da equação (3.3.3) e o fato de que $x_g \neq 0$ temos que $R x_g R$ é um ideal graduado próprio de R, uma contradição. Assim, $J = 0$. Como a dimensão de R é finita, segue que R é semissimples. □

3.4 Teorema de descrição

Esta seção será inteiramente dedicada a demonstrar o seguinte teorema de descrição, referente ao artigo [3]:

Teorema 3.4.1. *Seja $R = \bigoplus_{g \in G} R_g$ uma F-álgebra G-graduada de dimensão finita tal que F é um corpo algebricamente fechado. Suponha ainda que a ordem de cada subgrupo finito de G é invertível em F. Então R é uma álgebra graduada simples se, e somente se, R é isomorfa ao produto tensorial $M_q(F) \otimes F^\sigma[H] \cong M_q(F^\sigma[H])$, onde H é um subgrupo finito de G e $\sigma : H \times H \to F^*$ é um 2-cociclo em H. A graduação, com respeito a H em $F^\sigma[H]$ é canônica, a G-graduação em $M_q(F)$ é elementar definida por uma q-upla $(g_1, \ldots, g_q) \in G^q$ e considera-se a graduação em $M_q(F) \otimes F^\sigma[H]$ a graduação induzida pelo produto tensorial definida no exemplo 2.2.9.*

Note que $C = M_q(F) \otimes F^\sigma[H]$ é G-graduada simples. De fato, se $I \subset C$ é um ideal graduado não nulo então seja $u = E_{ij} \otimes r_h$ elemento homogêneo de grau g em I (podemos assumir que I contém u usando que dado um elemento $a \otimes b$ em I, podemos multiplicar à direita e esquerda por elementos do tipo $E_{st} \otimes 1$, que ainda "permanecemos"em I). Denote por 1 a identidade de $F^{\sigma}[H]$. Então, multiplicando à esquerda e à direita de u por $E_{st} \otimes 1$ teremos que $E_{ii} \otimes r_h \in I$ para todo $i = 1, \ldots, q$. Logo $Id \otimes r_h \in I$, pois I é subespaço. Como r_h é invertível segue que $Id \otimes 1 \in I$, o que mostra que $I = C$. Só nos falta provar a outra implicação.

Durante toda esta seção, as notações serão fixadas, para que a demonstração não se torne muito longa e enfadonha. Antes disso veremos dois lemas técnicos:

Lema 3.4.2. *Seja $B = B_1 \oplus \cdots \oplus B_n$ uma soma direta de álgebras de matrizes e $z_1, z_2 \in B$ dois idempotentes ortogonais. Considere*

$$z_1 = \sum_{j=1}^{n} z_1^j \text{ e } z_2 = \sum_{j=1}^{n} z_2^j$$

com $z_1^j, z_2^j \in B_j$. Então

$$dim(z_1 B z_2) = \sum_{j=1}^{n} (posto\ z_1^j)(posto\ z_2^j).$$

Demonstração. Fixado j, temos que z_1^j e z_2^j são idempotentes ortogonais. Sejam $m =$ *posto* z_1^j e $k =$ *posto* z_2^j. Suponha $B_j = M_p(F)$. Observe que z_1^j é semelhante à sua matriz escalonada $(z_1^j)'$. Além disso, *posto* $(z_1^j)' = m$. Logo

$$(z_1^j)' = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,m-1} & a_{1m} & a_{1,m+1} & \cdots & a_{1p} \\ 0 & a_{22} & \cdots & a_{2,m-1} & a_{2m} & a_{2,m+1} & \cdots & a_{2p} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{mm} & a_{m,m+1} & \cdots & a_{mp} \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Como $a_{ii} = 1$ e z_1^j é idempotente, segue que

$$z_1^j = E_{11} + \cdots + E_{mm}$$

Do mesmo modo, usando também que z_1^j e z_2^j são idempotentes ortogonais, mostra-se que z_2^j é semelhante à $E_{m+1,m+1} + \cdots + E_{m+k,m+k}$. Portanto

$$dim\ z_1^j B_j z_2^j = mk = (posto\ z_1^j)(posto\ z_2^j).$$

Da igualdade

$$z_1 B z_2 = \bigoplus_{j=1}^{n} z_1^j B_j z_2^j$$

segue o resultado. □

Lema 3.4.3. *Seja $R = \oplus_{g\in G} R_g$ uma álgebra graduada simples de dimensão finita sobre um corpo algebricamente fechado F tal que char $F = 0$ ou char F é coprima com a ordem de cada subgrupo finito de G. Assuma que a componente identidade de R é soma de dois somandos simples: $R_e = A_1 \oplus A_2$. Sejam $e_1 \in A_1$ e $e_2 \in A_2$ as identidades das álgebras A_1 e A_2, respectivamente. Denote $R_1 = e_1 R e_1$ e $R_2 = e_2 R e_2$. Pelos lemas* (3.3.3) *e* (3.3.4)*, podemos considerar as decomposições $R_1 = A_1 C_1$ e $R_2 = A_2 C_2$, onde C_1 e C_2 são álgebras de divisão graduadas. Sejam $d_1 \in A_1$ e $d_2 \in A_2$ um par de idempotentes minimais tais que $M = d_1 R d_2 \neq 0$. Então*

$$dim(C_1) = dim(M) = dim(C_2),$$
$$M = C_1 x = x C_2 \text{ para qualquer homogêneo } x,\ 0 \neq x \in M.$$

Demonstração. Pelo teorema (3.3.5), R é semissimples. Seja $R = B_1 \oplus \cdots \oplus B_n$ uma decomposição de R em soma de ideais simples. Podemos então escrever

$$e_1 = e_1^1 + \cdots + e_1^n, \quad e_1^i \in B_i, i = 1, \ldots, n.$$

Assim,

$$A_1 C_1 = R_1 = e_1 R e_1 = e_1^1 B_1 e_1^1 \oplus \cdots \oplus e_1^n B_n e_1^n. \tag{3.4.1}$$

Como C_1 é o centralizador de A_1 em R_1, segue que $C_1 = C_1^1 \oplus \cdots \oplus C_1^n$, onde $C_1^i = C_1 \cap B_i$.

De fato, dado $x = x_1 + \cdots + x_n \in C_1$, com $x_i \in B_i$, como C_1 é subálgebra graduada e $A_1 \subset R_e$, segue que $x_i \in C_1$ e a igualdade é verdadeira.

Fixe índice i, $1 \leq i \leq n$, denote por φ_i a projeção canônica de R sobre B_i e seja $A_1^i = \varphi_i(A_1)$. Observe que φ_i é um homomorfismo de álgebras. Considere a restrição $\varphi_i : A_1 \to B_i$. Como A_1 é simples, segue pelo teorema do isomorfismo que $A_1^i = 0$ ou $A_1^i \cong A_1$. Se $A_1^i = 0$, então

$$A_1 \subset \oplus B_1 \oplus \cdots B_{i-1} \oplus B_{i+1} \oplus \cdots \oplus B_n = R' \neq R.$$

Assim, o ideal RA_1R é graduado (pois é gerado por elementos homogêneos) e próprio, uma contradição. Assim, devemos ter $A_1^i \cong A_1$ e então C_1^i comuta com A_1^i.

Denote agora $B_i' = e_1^i B_i e_1^i$. Como $e_1^i = \varphi_i(e_1)$ é um idempotente e B_i é simples, segue que B_i' é simples. Além disso, $C_1^i \subset B_i'$. Note que $B_i' = A_1^i C_1^i$. De fato, pela igualdade (3.4.1), segue que

$$B_i' = e_1^i B_i e_1^i = \varphi_i(A_1 C_1) = \varphi_i(A_1)\varphi_i(C_1) = A_1^i C_1^i.$$

Observe ainda que C_1^i é simples, caso contrário, se $I \subset C_1^i$ é um ideal próprio de C_1^i então $B_i'I$ é um ideal próprio em B_i', uma contradição. Assim, $C_1^i \cong M_{p_i}(F)$, para algum $p_i \geq 1$ e

$$B_i' \cong A_1^i \otimes C_1^i \tag{3.4.2}$$

Considere a decomposição $d_1 = d_1^1 + \cdots + d_1^n$, com $d_1^j \in B_j$. Então, $d_1^i = \varphi_i(d_1)$ é um idempotente minimal de A_1^i e pela igualdade (3.4.2) o posto da matriz d_1^i em B_i' é p_i. Observe que $B_i' \subset B_i$ são duas álgebras de matrizes e $B_i' = e_1^i B_i e_1^i$, onde e_1^i é um idempotente. Assim, para qualquer matriz $x \in B_i'$, o posto de x em B_i' coincide com o posto de x em B_i. Deste modo *posto* $d_1^i = p_i$.

De modo análogo, denotando $C_2^j = C_2 \cap B_j$, $j = 1, \ldots, n$, tem-se

$$C_2 = C_2^1 \oplus \cdots + C_2^n, \quad C_2^j = M_{q_j}, \text{ com } q_j \geq 1, j = 1, \ldots, n$$

$$d_2 = d_2^1 + \cdots + d_2^n, \quad d_2^j \in B_j, \quad j = 1, \ldots, n$$

e *posto* $d_2^j = q_j$. Pelo lema (3.4.2),

$$dim(M) = \sum_{i=1}^{n} (posto\ d_1^i)(posto\ d_2^i) = \sum_{i=1}^{n} p_i q_i \tag{3.4.3}$$

e

$$dim\ C_1 = p_1^2 + \cdots + p_n^2, \qquad dim\ C_2 = q_1^2 + \cdots + q_n^2 \tag{3.4.4}$$

Agora note que $M = d_1 R d_2$ é um C_1-módulo à esquerda. De fato, essa observação segue do fato de que $d_1 \in A_1$ e C_1 comuta com os elementos de A_1. Como C_1 é uma álgebra de divisão graduada simples e M é um C_1-módulo à esquerda não trivial graduado, temos que $dim(M) \geq dim(C_1)$. Do mesmo modo, olhando M como um C_2-módulo à direita, tem-se $dim\ M \geq dim\ C_2$. Usando essas informações juntamente com as desigualdades (3.4.3) e (3.4.4) obtemos

$$p_1 q_1 + \cdots + p_n q_n \geq p_1^2 + \cdots + p_n^2,$$
$$p_1 q_1 + \cdots + p_n q_n \geq q_1^2 + \cdots + q_n^2$$

ou, equivalentemente, $\sum_i (p_1 - q_1)^2 \leq 0$. Portanto $p_1 = q_1, \cdots, p_n = q_n$, isto é, $dim(C_1) = dim(M) = dim(C_2)$.

Tome agora um elemento homogêneo arbitrário não nulo $x \in M$. Defina a transformação linear $\beta : C_1 \to C_1 x$ por $\beta(c) = cx$. Observe que β é injetora pois caso contrário existiria um homogêneo não nulo (e portanto invertível) $c \in C_1$ tal que $cx = 0$, uma contradição. Assim, $dim(M) = dim(C_1) = dim(C_1 x)$. Como $C_1 x \subset M$ (pois se $x = d_1 r d_2$ então $C_1 x = C_1 d_1 r d_2 = d_1 C_1 r d_2 \subset M$), segue que $C_1 x = M$. Do mesmo modo $x C_2 = M$ e terminamos. □

Trabalharemos com uma álgebra G-graduada simples R de dimensão finita sobre um corpo algebricamente fechado F tal que $char(F) = 0$ ou $char(F)$ é coprimo com a ordem de cada subgrupo finito de G. Pelo corolário (3.3.2) R_e é semissimples então escreveremos

$$R_e = A^{(1)} \oplus \cdots \oplus A^{(k)},$$

onde $A^{(j)} \cong M_{q_j}(F)$ com $q_j \geq 1$ para $j = 1, \ldots, k$. Denote por e_i a identidade de $A^{(i)}$.

Pelo lema (3.3.3), a subálgebra

$$R^{(i)} = e_i R e_i$$

é graduada simples. Denotaremos por $C^{(i)}$ o centralizador de $A^{(i)}$ em $R^{(i)}$.

Proposição 3.4.4. *O centralizador $C^{(i)}$ é uma subálgebra G graduada simples de R.*

Demonstração. Pelo lema (3.3.4), temos que $R^{(i)} = A^{(i)}C^{(i)} \cong A^{(i)} \otimes C^{(i)} \cong M_{q_i}(C^{(i)})$. Note que $C^{(i)}$ é subálgebra graduada de R. De fato, dado $c = c_1 + \cdots + c_n \in C^{(i)}$ com $c_j \in R_{g_j}$ para $j = 1, \ldots, n$ e $a \in A^{(i)} \subset R_e$ vale que $ca = ac$. Como $deg(c_j a) = g_j = deg(ac_j)$, temos que $ac_j = c_j a$, o que implica que $c_j \in C^{(i)}$ para todo $j = 1, \ldots, n$. Portanto $C^{(i)}$ é subálgebra graduada de R.

Considere agora I um ideal graduado de $C^{(i)}$ não trivial. Afirmamos que $A^{(i)}I$ é um ideal não trivial graduado de $R^{(i)}$. Primeiro observe que dados $u = \sum_j a_j c_j \in A^{(i)}C^{(i)} = R^{(i)}$ e $v = \sum_k a'_k d_k \in A^{(i)}I$, com $a'_k \in A^{(i)}$ e $d_k \in I$ temos

$$uv = \sum_{j,k} a_j c_j a'_k d_k = \sum_{j,k} a_j a'_k c_j d_k \in A^{(i)}I$$

pois c_j comuta com a'_k e I é ideal de $C^{(i)}$. Do mesmo modo mostra-se que $vu \in A^{(i)}I$. Mostremos agora que $A^{(i)}$ é graduado. Tome $ad \in A^{(i)}I$ com $a \in A^{(i)}$ e $d \in I$. Como I é graduado em $C^{(i)}$, podemos escrever $d = d_1 + \cdots + d_s$, com $d_j \in C^{(i)}_{h_j} \cap I$, $j = 1, \ldots, s$. Assim,

$$ad = ad_1 + \cdots, ad_s \in \bigoplus_{g \in G} A^{(i)}I \cap R_g$$

pois $deg(ad_j) = deg(a)deg(d_j) = h_j$. Caso tomarmos $u = \sum_l a_l d_l \in A^{(i)}I$, teremos pelo mesmo argumento, $u \in \bigoplus_{g \in G} A^{(i)}I \cap R_g$. Portanto $A^{(i)}I$ é ideal graduado de $R^{(i)}$. Como I é não trivial em $C^{(i)}$ e $A^{(i)}C^{(i)} = R^{(i)}$, segue que $A^{(i)}I$ é não trivial em $R^{(i)}$, o que é um absurdo. Portanto $C^{(i)}$ é graduada simples. □

De agora em diante, denotaremos $H^{(i)} = supp(C^{(i)})$.

Proposição 3.4.5. *A subálgebra $C^{(i)}$ é álgebra graduada de divisão e, portanto, $H^{(i)}$ é subgrupo de G.*

Demonstração. Note que $dim(A^{(i)} \cap C^{(i)}) = dim(Z(A^{(i)})) = 1$. Portanto,

$$dim(C_e^{(i)}) = dim(C^{(i)} \cap R_e) = dim(C^{(i)} \cap A^{(i)}) = 1$$

Pela proposição (3.3.2), $C^{(i)}$ é álgebra de divisão graduada. Pelo lema (3.2.1) $H^{(i)}$ é subgrupo de G. □

Denotaremos por

$$e_{\alpha,\beta}^{(i)},\ 1 \leq \alpha, \beta, \leq q_i$$

as matrizes unitárias de $A^{(i)}$. Neste caso, temos que

$$e_i = e_{11}^{(i)} + e_{22}^{(i)} + \cdots + e_{q_iq_i}^{(i)}.$$

Lema 3.4.6. *Mantidas as notações, temos que* $supp(C^{(i)}) = supp(R^{(i)})$, *para* $i = 1, \ldots, k$.

Demonstração. Como $R^{(i)} = A^{(i)}C^{(i)}$ e $A^{(i)} \subset R_e$, temos que todo elemento $r \in R^{(i)}$ se escreve na forma

$$r = \sum_l a_l c_l$$

com $a_l \in A^{(i)}$ e $c_l \in C^{(i)}$. Tome $h \in supp(C^{(i)})$. Então existe um homogêneo não nulo $c \in C_h^{(i)}$. Assim, o elemento $c = e_i c \in A^{(i)}C^{(i)} = R^{(i)}$. Assim, $H^{(i)} \subset supp(R^{(i)})$. Reciprocamente, tome $h \in supp(R^{(i)})$. Então existe um homogêneo não nulo $r = \sum_l a_l c_l \in R_h^{(i)}$. Como $deg(a_l) = e$ devemos ter $deg(c_l) = h$, para todo índice l. Como $r \neq 0$, devemos ter algum c_l não nulo e então, $h \in C_h^{(i)}$. Assim $supp(R^{(i)}) \subset H^{(i)}$. □

Proposição 3.4.7. *Fixe um inteiro m tal que $2 \leq m \leq k$. Então existem elementos homogêneos $\overline{x}_{i,i-1} \in e_iRe_{i-1}$ e $x_{i-1,i} \in e_{i-1}Re_i$, com $i = 2, \ldots, m$ tais que*

$$e_m\overline{x}_{m,m-1}e_{m-1} \cdots e_2\overline{x}_{2,1}e_1x_{12}e_2 \cdots e_{m-1}x_{m-1,m}e_m \neq 0$$

satisfazendo $deg(\overline{x}_{i,i-1}x_{i-1,i}) = e$.

Demonstração. Primeiro note que

$$W_m = e_mRe_{m-1}R \cdots e_2Re_1Re_2R \cdots e_{m-1}Re_m = R^{(m)}.$$

Provemos essa afirmação por indução em m. Se $m = 2$, então note que Re_1R é um ideal não nulo graduado de R (pois é gerado por um elemento homogêneo). Logo $Re_1R = R$. Assim,

$$W_2 = e_2Re_1Re_2 = e_2Re_2 = R^{(2)}.$$

Suponha agora que $W_{m-1} = R^{(m-1)}$. Assim, W_{m-1} é homogêneo. Assim, o ideal $RW_{m-1}R$ é graduado em R e portanto, $RW_{m-1}R = R$. Assim,

$$W_m = e_mRW_{m-1}Re_m = e_mRe_m = R^{(m)}$$

como queríamos. Portanto, $W_m = R^{(m)} \neq 0$ e então existem homogêneos $\overline{x}_{i,i-1} \in e_iRe_{i-1}$ e $x_{i-1,i} \in e_{i-1}Re_i$ tais que

$$w_m = e_m\overline{x}_{m,m-1}e_{m-1} \cdots e_2\overline{x}_{2,1}e_1x_{12}e_2 \cdots e_{m-1}x_{m-1,m}e_m \neq 0. \tag{3.4.5}$$

Para cada índice j tal que $2 \leq j \leq m$, denote por w_j o fator

$$e_j\overline{x}_{j,j-1} \cdots e_2\overline{x}_{21}e_1x_{12} \cdots e_{j-1}x_{j-1,j}e_j$$

que aparece em (3.4.5). Se $deg(w_2) = h \neq e$ então pelo lema (3.4.6) temos que

$$h \in supp(R^{(2)}) = H^{(2)}.$$

Como $H^{(2)}$é subgrupo, segue que $h^{-1} \in H^{(2)}$. Tome então um elemento homogêneo não nulo $b \in C^{(2)}$ tal que $deg(b) = h^{-1}$. Assim, considerando o elemento $\overline{x}'_{21} = b\overline{x}_{21}$, temos que

$$w'_2 = e_2\overline{x}'_{21}e_1x_{12}e_2 = e_2b\overline{x}_{21}e_1x_{12}e_2 = be_2\overline{x}_{21}e_1x_{12}e_2 = bw_2,$$

onde usamos que b comuta com e_2. Note agora que $w'_2 \neq 0$ pois b é invertível ($C^{(2)}$ é álgebra graduada de divisão pela proposição (3.4.5)) e $w_2 \neq 0$. Além disso, $deg(w'_2) = deg(b)deg(w_2) = e$, como queríamos. De modo geral, suponha que já tenhamos feito esse processo até o índice $m-1$. Temos que $\overline{x}_{m,m-1}x_{m-1,m} \in R^{(m)}$. Caso $deg(\overline{x}_{m,m-1}x_{m-1,m}) = g \neq e$ então $g \in supp(R^{(m)}) = H^{(m)}$. Como $H^{(m)}$ é subgrupo de G, tome um homogêneo não nulo $d \in C^{(m)}$ tal que $deg(d) = g^{-1}$. Considerando o elemento $\overline{x}'_{m,m-1} = d\overline{x}_{m,m-1}$, temos que

$$\begin{aligned} w'_m &= e_m \overline{x}'_{m,m-1} e_{m-1} \cdots e_2 \overline{x}_{21} e_1 x_{12} \cdots e_{m-1} x_{m-1,m} \\ &= e_m d\overline{x}_{m,m-1} e_{m-1} \cdots e_2 \overline{x}_{21} e_1 x_{12} \cdots e_{m-1} x_{m-1,m} \\ &= d e_m \overline{x}_{m,m-1} e_{m-1} \cdots e_2 \overline{x}_{21} e_1 x_{12} \cdots e_{m-1} x_{m-1,m} \\ &= d w_m. \end{aligned}$$

Note que $w'_m \neq 0$ pois $w_m \neq 0$ e d é invertível. Como,

$$\begin{aligned} deg(w'_m) &= deg(d)deg(w_m) \\ &= deg(d)deg(e_m \overline{x}_{m,m-1} w_{m-1} x_{m-1,m} e_m) \\ &= deg(d)deg(\overline{x}_{m,m-1} x_{m-1,m}) \\ &= e \end{aligned}$$

a proposição está demonstrada. □

Considere os elementos homogêneos do enunciado da proposição (3.4.7) (considerando $m = k$). Observe que para $i = 1, \ldots, k-1$, vale

$$\begin{aligned} \overline{x}_{i+1,i} x_{i,i+1} &\in R_e \cap R^{(i+1)}, \\ x_{i,i+1} \overline{x}_{i+1,i} &\in R_e \cap R^{(i)}. \end{aligned}$$

Como

$$e_k \overline{x}_{k,k-1} e_{k-1} \cdots e_2 \overline{x}_{2,1} e_1 x_{12} e_2 \cdots e_{k-1} x_{k-1,k} e_k \neq 0$$

existem índices $\alpha_1, \ldots, \alpha_k, \beta_2, \ldots, \beta_k$ com $1 \leq \alpha_j, \beta_j \leq q_j$, para $j = 1, \ldots, k$ tais que

$$e^{(k)}_{\beta_k,\beta_k} \overline{x}_{k,k-1} e^{(k-1)}_{\beta_{k-1}\beta_{k-1}} \cdots e^{(2)}_{\beta_2,\beta_2} \overline{x}_{21} e^{(1)}_{\alpha_1,\alpha_1} x_{12} \cdots e^{(k-1)} x_{k-1,k} e^{(k)}_{\alpha_k,\alpha_k} \neq 0 \tag{3.4.6}$$

Defina agora os elementos homogêneos para $i = 1, \ldots, k-1$

$$\begin{aligned} y_{i,i+1} &= e^{(i)}_{1,\alpha_i} e^{(i)}_{\alpha_i,\alpha_i} x_{i,i+1} e^{(i+1)}_{\alpha_{i+1},\alpha_{i+1}} e^{(i+1)}_{\alpha_{i+1},1}, \\ y_{i+1,i} &= e^{(i+1)}_{1,\beta_{i+1}} e^{(i+1)}_{\beta_{i+1},\beta_{i+1}} \overline{x}_{i+1,i} e^{(i)}_{\beta_i,\beta_i} e^{(i)}_{\beta_i,1}. \end{aligned}$$

Note que todos os $y_{i,i+1}, y_{i+1,i}$ são homogêneos e satisfazem

$$e^{(i)}_{11} y_{i,i+1} e^{(i+1)}_{11} = y_{i,i+1}, \; e^{(i+1)}_{11} y_{i+1,i} e^{(i)}_{11} = y_{i+1,i}. \tag{3.4.7}$$

Além disso, segue de (3.4.6) que

$$y_{k,k-1} y_{k-1,k-2} \cdots y_{21} y_{12} y_{23} \cdots y_{k-1,k} \neq 0. \tag{3.4.8}$$

Defina agora os seguintes elementos: se $1 \leq i < j \leq k$,

$$y_{ij} = y_{i,i+1} y_{i+1,i+2} \cdots y_{j-1,j}, \quad y_{ji} = y_{j,j-1} y_{j-1,j-2} \cdots y_{i+1,i}. \tag{3.4.9}$$

Note que as igualdades em (3.4.7) são verdadeiras agora para quaisquer índices i, j pois se $1 \leq i < j \leq k$ então

$$\begin{aligned} e^{(i)}_{11} y_{ij} e^{(j)}_{11} &= e^{(i)}_1 1 e^{(i)}_1 1 y_{i,i+1} e^{(i+1)}_{11} e^{(i+1)}_{11} y_{i+1,i+2} e^{(i+2)}_{11} \cdots e^{(j-1)}_{11} y_{j-1,j} e^{(j)}_{11} e^{(j)}_{11} \\ &= e^{(i)}_1 1 y_{i,i+1} e^{(i+1)}_{11} e^{(i+1)}_{11} y_{i+1,i+2} e^{(i+2)}_{11} \cdots e^{(j-1)}_{11} y_{j-1,j} e^{(j)}_{11} \\ &= y_{i,i+1} y_{i+1,i+2} \cdots y_{j-1,j} \\ &= y_{ij}. \end{aligned}$$

De modo análogo mostra-se que $e^{(j)}_{11} y_{ji} e^{(i)}_{11} = y_{ji}$. Portanto temos a relação:

$$e^{(i)}_{11} y_{ij} e^{(j)}_{11} = y_{ij}, \; 1 \leq i, j, \leq k. \tag{3.4.10}$$

Vamos agora definir elementos que denotaremos por $y_{11}, y_{22}, \ldots, y_{kk}$. Considere primeiramente $y_{22} = y_{21} y_{12}$. Note que em virtude da igualdade (3.4.8) e da proposição

(3.4.7) temos que $y_{22} \neq 0$ e $deg(y_{22}) = deg(y_{21}y_{12}) = deg(\overline{x}_{21}x_{12}) = e$. Assim

$$y_{22} \in R_e \cap R^{(2)} = (R^{(2)})_e \subset A^{(2)},$$

onde a última inclusão é verdadeira uma vez que se $y_{22} = a_1 + \cdots + a_k$, com $a_j \in A^{(j)}$, segue que

$$y_{22} = e_2 y_{22} e_2 = e_2 a_2 e_2 \in A^{(2)}.$$

Assim, y_{22} é uma matriz em $A^{(2)}$. Como $e_{11}^{(2)} y_{22} e_{11}^{(2)} = y_{22}$ temos então que y_{22} deve ser múltiplo escalar da matriz $e_{11}^{(2)}$, isto é, $y_{22} = \lambda e_{11}^{(2)}$, para algum $\lambda \in F$ não nulo. Se trocarmos y_{21} por $\lambda^{-1} y_{21}$, as relações em (3.4.9) e (3.4.10) permanecem válidas. Deste modo, podemos assumir $y_{22} = e_{11}^{(2)}$. Até mais.

Considere agora $y_{11} = y_{12}y_{21}$. Pelo mesmo argumento acima, devemos ter $y_{11} = \alpha e_{11}^{(1)}$, para algum $\alpha \in F$. Note que $(y_{11})^2 = \alpha y_{11}$. Assim,

$$\begin{aligned}
(y_{22})^3 &= y_{21}y_{12}y_{21}y_{12}y_{21}y_{12} \\
&= y_{21}(y_{11})^2 y_{12} \\
&= y_{21}(\alpha y_{11}) y_{12} \\
&= \alpha y_{21} y_{11} y_{12} \\
&= \alpha y_{21} y_{12} y_{21} y_{12} \\
&= \alpha (y_{22})^2 \\
&= \alpha y_{22}
\end{aligned}$$

pois $y_{22} = e_{11}^{(1)}$ é nilpotente. Por outro lado, $(y_{22})^3 = y_{22}$. Disso concluímos que $\alpha = 1$ e portanto $y_{11} = e_{11}^{(1)}$. O mesmo processo, substituindo $y_{i+1,i}$ por um múltiplo escalar conveniente de $y_{i+1,i}$, nos fornece

$$y_{i,i+1}y_{i+1,i} = e_{11}^{(i)}, \quad y_{i+1,i}y_{i,i+1} = e_{11}^{(i+1)}$$

enquanto que as relações (3.4.9) e (3.4.10) permanecem válidas. Assim, definimos $y_{ii} = e_{11}^{(i)}$, para $i = 1, \ldots, k$.

Proposição 3.4.8. *Os elementos y_{ij}, $1 \leq i, j \leq k$ definidos acima satifazem*

$$y_{ij}y_{kl} = \delta_{jk}y_{il},$$

onde δ_{ij} é o delta de Kronecker. Consequentemente tais elementos formam um conjunto linearmente independente.

Demonstração. Fixe índices i, j, s, t. Note que se $j \neq s$, usando (3.4.10) obtemos

$$y_{ij}y_{st} = e_{11}^{(i)}y_{ij}e_{11}^{(j)}e_{11}^{(s)}y_{st}e_{11}^{(t)} = 0$$

pois $e_{11}^{(j)}e_{11}^{(s)} = 0$ e a proposição é verdadeira. Passemos ao caso em que $j = s$. Se $i < j < t$ ou $i > j > t$ a proposição segue da definição (3.4.9).

Se $i = j < t$ então

$$\begin{aligned}
y_{ii}y_{is} &= e_{11}^{(i)}y_{i,i+1}y_{i+1,s} \\
&= e_{11}^{(i)}(e_{1,\alpha_i}^{(i)}e_{\alpha_i,\alpha_i}^{(i)}x_{i,i+1}e_{\alpha_{i+1},\alpha_{i+1}}^{(i+1)}e_{\alpha_{i+1},1}^{(i+1)})y_{i+1,s} \\
&= e_{1,\alpha_i}^{(i)}e_{\alpha_i,\alpha_i}^{(i)}x_{i,i+1}e_{\alpha_{i+1},\alpha_{i+1}}^{(i+1)}e_{\alpha_{i+1},1}^{(i+1)}y_{i+1,s} \\
&= y_{i,i+1}y_{i+1,s} \\
&= y_{i,s}.
\end{aligned}$$

Se $i = j > t$ ou $i < j = t$ usa-se argumento análogo ao acima. Se $i < j$ e $j > t$, temos

$$\begin{aligned}
y_{ij}y_{jt} &= (y_{i,i+1}\cdots y_{j-2,j-1}y_{j-1,j})(y_{j,j-1}y_{j-1,j-2}\cdots y_{t+1,t}) \\
&= y_{i,i+1}\cdots y_{j-2,j-1}e_{11}^{(j-1)}y_{j-1,j-2}\cdots y_{t+1,t} \\
&= y_{i,i+1}\cdots e_{11}^{(j-1)}y_{j-2,j-1}e_{11}^{(j-1)}e_{11}^{(j-1)}e_{11}^{(j-1)}y_{j-1,j-2}e_{11}^{(j-2)}\cdots y_{t+1,t} \\
&= y_{i,i+1}\cdots y_{j-2,j-1}y_{j-1,j-2}\cdots y_{t+1,t} \\
&= y_{i,j-1}y_{j-1,t}
\end{aligned}$$

Agora utilizamos o mesmo argumento em $y_{i,j-1}$ e $y_{j-1,t}$ até cairmos num dos casos $y_{ii}y_{it}$ ou $y_{it}y_{tt}$. Daí segue de um dos casos anteriores.

Se $i > j$ e $j < t$ então usa-se um argumento de "redução" análogo ao acima. Portanto a proposição está provada. □

Proposição 3.4.9. *O subespaço S de R com base*

$$\{y_{ij} \ : 1 \leq i, j \leq k\}$$

é uma subálgebra graduada de R. Além disso, S é isomorfo a $M_k(F)$ e existem $e = g_1, g_2, \ldots, g_k \in G$ tais que $deg(y_{ij}) = g_i g_j^{-1}$.

Demonstração. S é graduada pois é gerada por elementos homogêneos de R. O fato de que $S \cong M_k(F)$ segue da aplicação $\eta : S \to M_k(F)$ que associa y_{ij} à matriz elementar $E_{ij} \in M_k(F)$. Agora note que $y_{ii} = e_{11}^{(i)} \in A^{(i)} \subset R_e$, isto é, todas as matrizes y_{ii} são homogêneas. Pelo lema (2.2.6) segue a proposição. □

Considere agora o idempotente $t = e_i + e_j$, $i \neq j$. Pelo lema (3.3.3) $R' = tRt$ é graduada simples e

$$(R')_e = R' \cap R_e = (e_i + e_j)R(e_i + e_j) \cap (A^{(1)}) \oplus \cdots \oplus A^{(k)} = A^{(i)} \oplus A^{(j)}.$$

Observe ainda que $C^{(i)}$ é o centralizador de $A^{(i)}$ em $e_iRe_i = e_iR'e_i$. Como y_{ij} é homogêneo não nulo vale que

$$C^{(i)} y_{ij} = y_{ij} C^{(j)}. \tag{3.4.11}$$

Lema 3.4.10. *Para cada $x \in C^{(i)}$ homogêneo, existe único $x' \in C^{(j)}$ tal que $xy_{ij} = y_{ij}x'$.*

Demonstração. A existência é garantida pela igualdade (3.4.11). Além disso, se

$$xy_{ij} = y_{ij}x'$$

com x homogêneo, então como y_{ij} é homogêneo segue que x' também o é. De fato, se $x' = x'_1 + \cdots + x'_m$ com $x'_s \in R_{g_s}$, temos que

$$y_{ij}x' = \sum_s y_{ij}x'_s$$

é homogêneo. Daí devemos ter $m = 1$. Suponha agora que existam $x', x'' \in C^{(j)}$ tais que

$$xy_{ij} = y_{ij}x' = y_{ij}x''.$$

Como $x' - x''$ é homogêneo, se $x' \neq x''$ obteremos $y_{ij} = 0$ uma vez que $C^{(j)}$ é álgebra graduada de divisão. Portanto $x' = x''$ e o lema está provado. □

A partir do lema anterior, podemos definir uma função

$$\varphi : C^{(i)} \to C^{(j)} \tag{3.4.12}$$

onde para cada $x \in C^{(i)}$ homogêneo, $\varphi(x)$ seja o único elemento x' tal que (3.4.11) seja válido. Observe ainda que se $x, y \in C^{(i)}$ são homogêneos, então

$$xyy_{ij} = xy_{ij}\varphi(y) = y_{ij}\varphi(x)\varphi(y),$$

isto é, $\varphi(xy) = \varphi(x)\varphi(y)$. Além disso, se φ não é injetora, então existe um homogêneo não nulo $x \in C^{(i)}$ tal que $\varphi(x) = 0$. Mas então $xy_{ij} = 0$, o que implica $y_{ij} = 0$, um absurdo. Como $dimC^{(i)} = dimC^{(j)}$ pelo lema (3.4.3), temos que a aplicação φ é um isomorfismo de álgebras.

Observe ainda o seguinte: se $x \in C^{(i)}$ é homogêneo, então

$$deg(\varphi(x)) = (deg(y_{ij}))^{-1}deg(x)deg(y_{ij}).$$

De fato, suponha $deg(x) = h$ e $deg(y_{ij}) = g$. Já vimos que $\varphi(x)$ é homogêneo. Então, devemos ter

$$hg = gdeg(\varphi(x)),$$

como queríamos.

Além disso, se denotarmos $deg(y_{ij}) = g$ então a aplicação

$$\eta : H^{(i)} \to H^{(j)}$$

dada por $\eta(h) = g^{-1}hg$ é um isomorfismo de grupos.

Para cada $i = 2, \ldots, k$, denote por $\varphi_i : C^{(1)} \to C^{(i)}$ o isomorfismo de álgebras definido em (3.4.12) e por $\varphi_1 = id_{C^{(1)}}$. Então

$$\varphi_1(x)y_{1i} = y_{1i}\varphi_i(x) \tag{3.4.13}$$

para todo $x \in C^{(1)}$ e $i = 1, \ldots, k$.

Proposição 3.4.11. *Com as notações acima, se $1 \leq i, j \leq k$, para todo $x \in C^{(1)}$ vale a igualdade*

$$\varphi_i(x)y_{ij} = y_{ij}\varphi_j(x). \tag{3.4.14}$$

Demonstração. Tome $x \in C^{(1)}$. O caso em que $i = j$ é imediato pois $y_{ii} = e_{11}^{(i)} \in A^{(i)}$ e $\varphi_i(x) \in C^{(i)}$, que é o centralizador de $A^{(i)}$. Suponha então $i < j$. Então por (3.4.13)

$$xy_{1i} = y_{1i}\varphi_i(x).$$

Logo

$$xy_{1j} = xy_{1i}y_{ij} = y_{1i}\varphi_i(x)y_{ij} \tag{3.4.15}$$

Por outro lado,

$$xy_{1j} = y_{1j}\varphi_j(x) = y_{1i}y_{ij}\varphi_j(x). \tag{3.4.16}$$

Multiplicando à esquerda de (3.4.15) e (3.4.16) por y_{i1} e lembrando que $y_{ii} \in A^{(i)}$ e $\varphi_i(x) \in C^{(i)}$, temos

$$y_{i1}y_{1i}\varphi_i(x)y_{ij} = y_{ii}\varphi_i(x)y_{ij} = \varphi_i(x)y_{ii}y_{ij} = \varphi_i(x)y_{ij}.$$

Por outro lado,

$$y_{i1}y_{1i}y_{ij}\varphi_j(x) = y_{ij}\varphi_j(x)$$

donde concluímos que $\varphi_i(x)y_{ij} = y_{ij}\varphi_j(x)$.

Suponha agora $i > j$. Para qualquer índice s tal que $2 \leq s \leq k$, tem-se

$$y_{11}x = xy_{11} = xy_{1s}y_{s1} = y_{1l}\varphi_s(x)y_{s1}.$$

Multiplicando à esquerda por y_{s1}, temos

$$y_{s1}x = y_{ss}\varphi_s(x)y_{s1} = \varphi_s(x)y_{ss}y_{s1} = \varphi_s(x)y_{s1}.$$

Usando a igualdade acima e o caso anterior, obtemos

$$\varphi_i(x)y_{ij} = \varphi_i(x)y_{i1}y_{1j} = y_{i1}xy_{1j} = y_{i1}y_{1j}\varphi_j(x) = y_{ij}\varphi_j(x)$$

como queríamos demonstrar. □

Lema 3.4.12. *Para cada $x \in C^{(1)}$, denote*

$$\overline{x} = x + \varphi_2(x) + \cdots + \varphi_k(x).$$

Então $C = span\{\overline{x} \ : x \in C^{(1)}\}$ é uma subálgebra de R isomorfa a $C^{(1)}$. Além disso,

$$\overline{x}z_i = \varphi_i(x)z_i, \quad z_i\overline{x} = z_i\varphi_i(x),$$

para qualquer $z_i \in e_iRe_i$, $i = 1, \ldots, k$.

Demonstração. Dados $\overline{x}, \overline{y} \in C$, com $x, y \in C^{(1)}$, note que como $\varphi_i(x) \in C^{(i)} \subset e_iRe_i$ e $\varphi_j(y) \in C^{(j)} \subset e_jRe_j$, se $i \neq j$ então $\varphi_i(x)\varphi_j(y) = 0$. Além disso, $x\varphi_j(y) = 0$, para $j = 2, \ldots, k$ e $\varphi_i(x)y = 0$, para $i = 2, \ldots, k$. Assim,

$$\begin{aligned} \overline{x}\,\overline{y} &= (x + \varphi_2(x) + \cdots + \varphi_k(x))(y + \varphi_2(y) + \cdots + \varphi_k(y)) && (3.4.17) \\ &= xy + \varphi_2(xy) + \cdots + \varphi_k(xy) && (3.4.18) \\ &= \overline{xy}. && (3.4.19) \end{aligned}$$

Logo C é uma subálgebra de R.

Considere a aplicação sobrejetora e F-linear:

$$\begin{array}{rcl} \delta : C^{(1)} & \longrightarrow & C \\ x & \longmapsto & \overline{x} \end{array}$$

Se $0 = \delta(x) = \overline{x}$ então $0 = e_1(x + \varphi_2(x) + \cdots + \varphi_k(x)) = x$, isto é, δ é um isomorfismo de álgebras. Finalmente, se $z_i \in e_iRe_i$ então

$$\overline{x}z_i = (x + \varphi_2(x) + \cdots + \varphi_k(x))z_i = \varphi_i(x)z_i,$$
$$z_i\overline{x} = z_i(x + \varphi_2(x) + \cdots + \varphi_k(x)) = z_i\varphi_i(x)$$

e o lema está provado. □

Considere agora os elementos da forma

$$e^{(i)}_{\alpha,1}y_{ij}e^{(j)}_{1,\beta} \tag{3.4.20}$$

com $1 \leq i, j \leq k$, $1 \leq \alpha \leq q_i$, $1 \leq \beta \leq q_j$. Tais elementos são homogêneos e não nulos. De fato, se $e^{(i)}_{\alpha,1}y_{ij}e^{(j)}_{1,\beta} = 0$ então

$$\begin{array}{rcl} 0 & = & e^{(i)}_{1,\alpha}e^{(i)}_{\alpha,1}y_{ij}e^{(j)}_{1,\beta}e^{(j)}_{\beta,1} \\ & = & e^{(i)}_{11}y_{ij}e^{(j)}_{11} \\ & = & y_{ij} \end{array}$$

o que é um absurdo. Além disso, os elementos de (3.4.20) são linearmente independentes.

Proposição 3.4.13. *Denote*

$$B = Span\{e^{(i)}_{\alpha,1}y_{ij}e^{(j)}_{1,\beta}\ : 1 \leq i, j \leq k;\ 1 \leq \alpha \leq q_i;\ 1 \leq \beta \leq q_j\}$$

e considere $q = q_1 + \cdots + q_k$. Então B é uma álgebra isomorfa a $M_q(F)$.

Demonstração. Considere o produto $\left(e^{(i)}_{\alpha,1}y_{ij}e^{(j)}_{1,\beta}\right)\left(e^{(s)}_{\gamma,1}y_{st}e^{(t)}_{1,\theta}\right)$. Se $j \neq s$ ou $\beta \neq \gamma$ então esse produto é nulo. Se $j = s$ e $\beta = \gamma$ então

$$\begin{aligned}\left(e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta}\right)\left(e^{(j)}_{\beta,1} y_{jt} e^{(t)}_{1,\theta}\right) &= e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{11} y_{jt} e^{(t)}_{1,\theta} \\ &= e^{(i)}_{\alpha,1} y_{ij} y_{jt} e^{(t)}_{1,\theta} \\ &= e^{(i)}_{\alpha,1} y_{it} e^{(t)}_{1,\theta} \in B\end{aligned}$$

isto é, B é de fato uma subálgebra. Defina então a aplicação

$$\psi : B \to M_q(F) \tag{3.4.21}$$

por $\psi\left(e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta}\right) = E_{\mu\nu}$, onde $\mu = q_1 + \cdots + q_{i-1} + \alpha$ e $\nu = q_1 + \cdots + q_{j-1} + \beta$. Pelo exposto acima, não é difícil ver que ψ preserva o produto. Além disso, dada $E_{\mu\nu} \in M_q(F)$, tome índices $1 \leq i, j \leq k$ tais que

$$\begin{aligned} q_1 + \cdots + q_{i-1} < \mu \text{ e } q_1 + \cdots + q_i \geq \mu, \\ q_1 + \cdots + q_{j-1} < \nu \text{ e } q_1 + \cdots + q_j \geq \nu. \end{aligned}$$

Tome agora índices $1 \leq \alpha \leq q_i$ e $1 \leq \beta \leq q_j$ tais que

$$q_1 + \cdots + q_{i-1} + \alpha = \mu \text{ e } q_1 + \cdots + q_{j-1} + \beta = \nu$$

Assim, temos que $\psi\left(e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta}\right) = E_{\mu\nu}$. Logo ψ leva a base em base e então é um isomorfismo de álgebras. □

Note que devido à proposição (3.4.11) e ao lema (3.4.12), se $\overline{x} \in C$ então

$$\begin{aligned}\overline{x} e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} &= \varphi_i(x) e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} \\ &= e^{(i)}_{\alpha,1} \varphi_i(x) y_{ij} e^{(j)}_{1,\beta} \\ &= e^{(i)}_{\alpha,1} y_{ij} \varphi_j(x) e^{(j)}_{1,\beta} \\ &= e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} \varphi_j(x) \\ &= e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} \overline{x}.\end{aligned}$$

Assim, C centraliza B em R. Além disso, $C \cap B = Z(B) \cong F$, e portanto o produto BC é isomorfo ao produto tensorial $B \otimes C$. Mostremos que $BC = R$. Fixe índices $1 \leq i, j \leq k$

e defina

$$P_{ij\alpha\beta} = Span\{e_{\alpha,1}^{(i)}C^{(i)}y_{ij}e_{1\beta}^{(j)}\}.$$

Observe que $P_{ij\alpha\beta} = C^{(i)}P_{ij\alpha\beta} = P_{ij\alpha\beta}C^{(j)}$. Consequentemente,

$$Q_{ij} = \sum_{1\leq\alpha\leq n_i \quad 1\leq\beta\leq n_j} P_{ij\alpha\beta} \subset e_iRe_j$$

é um $A^{(i)}C^{(i)}$-módulo à esquerda e um $A^{(j)}C^{(j)}$-módulo à direita. Afirmamos que $Q_{ij} = e_iRe_j$. Caso não valha a igualdade, então Q_{ij} gera um ideal graduado de R tal que

$$RQ_{ij}R \cap (e_iRe_j) = (e_iRe_i)Q_{ij}(e_jRe_j) = R^{(i)}Q_{ij}R^{(j)} = A^{(i)}C^{(i)}Q_{ij}A^{(j)}C^{(j)} = Q_{ij} \neq e_iRe_j$$

o que é uma contradição. Portanto $Q_{ij} = e_iRe_j$ e $BC = R$.

Portanto $R = BC \cong B \otimes C$. Vamos definir primeiro uma graduação em B. Pela proposição (3.4.9), a álgebra $S = Span\{y_{ij} \ : 1 \leq i, j \leq k\}$ é isomorfa e $M_k(F)$ e existem $g_1 = e, g_2, \ldots, g_k \in G$ tais que $deg(y_{ij}) = g_i^{-1}g_j$. Assim, para arbitrários $1 \leq i, j \leq k$ e $1 \leq \alpha \leq q_i$ e $1 \leq \beta \leq q_j$, vale que

$$deg\left(e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)}\right) = g_i^{-1}g_j.$$

Considere agora a q-upla

$$(\underbrace{g_1, \ldots, g_1}_{q_1}, \underbrace{g_2, \ldots, g_2}_{q_2}, \ldots, \underbrace{g_k, \ldots, g_k}_{q_k}) = (a_1, \ldots, a_q)$$

e que $M_q(F)$ tenha graduação elementar proveniente dessa q-upla, isto é, $deg(E_{\mu\nu}) = a_\mu^{-1}a_\nu$. Afirmamos que a aplicação $\psi : B \to M_q(F)$ definida em (3.4.21) é um isomorfismo de álgebras graduadas. De fato, tome $e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)} \in B_{g_i^{-1}g_j}$. Então $\psi\left(e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)}\right) = E_{\mu\nu}$. Logo $deg\left(\psi\left(e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)}\right)\right) = a_\mu^{-1}a_\nu$. Mas como $\mu = q_1 + m\cdots + q_{i-1} + \alpha$ e $\nu = q_1 + \cdots + q_{j-1} + \beta$, segue que $a_\mu = g_i$ e $a_\nu = g_j$. Portanto ψ é um isomorfismo de álgebras graduadas.

Lembre que $C^{(1)}$ é uma álgebra de divisão graduada. Considere-a com a graduação canônica. Considere também o produto tensorial $M_q(F)\otimes C^{(1)}$ com a graduação induzida.

Defina

$$\Phi : R = BC \longrightarrow M_q(F) \otimes C^{(1)}$$

por $\Phi\left(e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} \overline{x_h}\right) = \psi(e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta}) \otimes \delta^{-1}(\overline{x_h}) = E_{\mu\nu} \otimes x_h$, para cada $\overline{x_h} \in C$ com $deg(x_h) = h$. É claro que Φ é um isomorfismo de álgebras (pois ψ e δ o são). Mostremos que Φ preserva a graduação. Fixe índices $1 \leq i, j \leq k$, $1 \leq \alpha \leq q_i$, $1 \leq \beta \leq q_j$ e $\overline{x_h} \in C$ com $deg(x_h) = h$. Então por um lado,

$$deg(E_{\mu\nu} \otimes x_h) = a_\mu^{-1} h a_\nu = g_i^{-1} h g_j.$$

Por outro lado, embora o elemento $\overline{x_h}$ não seja homogêneo, temos que

$$\begin{aligned} \overline{x_h} e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} &= \varphi_i(x_h) e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta} \\ &= e^{(i)}_{\alpha,1} \varphi_i(x_h) y_{ij} e^{(j)}_{1,\beta} \end{aligned}$$

é homogêneo e

$$\begin{aligned} deg\left(\overline{x_h} e^{(i)}_{\alpha,1} y_{ij} e^{(j)}_{1,\beta}\right) &= deg(\varphi_i(x_h)) deg(y_{ij}) \\ &= deg(\varphi_i(x_h)) g_i^{-1} g_j \end{aligned}$$

Vamos calcular $deg(\varphi_i(x_h))$. Lembre que

$$x_h y_{1i} = y_{1i} \varphi_i(x_h).$$

Daí,

$$h g_1^{-1} g_i = deg(x_h y_{1i}) = deg(y_{1i} \varphi_i(x_h)) = g_1^{-1} g_i deg(\varphi_i(x_h))$$

Como $g_1 = e$, segue que $deg(\varphi_i(x_h)) = g_i^{-1} h g_i$. Finalmente,

$$\begin{aligned}
deg\left(\overline{x_h}e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)}\right) &= deg(\varphi_i(x_h))g_i^{-1}g_j \\
&= g_i^{-1}hg_ig_i^{-1}g_j \\
&= g_i^{-1}hg_j \\
&= deg(E_{\mu\nu}\otimes x_h) \\
&= deg\left(\Phi\left(\overline{x_h}e_{\alpha,1}^{(i)}y_{ij}e_{1,\beta}^{(j)}\right)\right).
\end{aligned}$$

Portanto, Φ é um isomorfismo de álgebras graduadas e o teorema (3.4.1) está provado.

Observamos que na demonstração do teorema (3.4.1), a decomposição obtida, que não é necessariamente única, é de tal forma que $R_e \cong A_e$. Isso se deve ao fato de termos $R = AC$ e $A \cong M_q(F)$. Como R_e é semissimples, escrevemos

$$R_e \cong \bigoplus_{i=1}^{k} M_{q_i}(F).$$

Além disso, obtivemos que $q = \sum_{i=1}^{k} q_i$ e $M_q(F)$ tem uma graduação definida por uma q-upla

$$(\underbrace{g_1,\ldots,g_1}_{q_1},\underbrace{g_2,\ldots,g_2}_{q_2},\ldots,\underbrace{g_k,\ldots,g_k}_{q_k}).$$

Portanto

$$R_e \cong \bigoplus_{i=1}^{k} M_{q_i}(F) \cong A_e.$$

Capítulo 4

PI-equivalência em álgebras graduadas simples

Sabemos que se duas álgebras G-graduadas são G-isomorfas então elas possuem as mesmas identidades graduadas. Porém, se põe a pergunta recíproca, isto é: Se duas álgebras G-graduadas possuem as mesmas identidades graduadas então elas são G-isomorfas? Este capítulo será dedicado à demonstração deste resultado para o caso de álgebras G-graduadas simples de dimensão finita sobre um corpo algebricamente fechado F tal que a ordem de cada subgrupo finito de G é invertível em F. Um dos pontos de partida será justamente o teorema de descrição (3.4.1). Usaremos as técnicas desenvolvidas nos artigos [1] e [19].

Considere a álgebra de matrizes $R = M_n(F)$ com uma G-graduação elementar definida por uma n-upla $(g_1, \ldots, g_n) \in G^n$. Pelo lema (2.2.7), podemos assumir, a menos de isomorfismo G-graduado, que R possui uma graduação proveniente de uma n-upla da forma

$$(\underbrace{g_{i_1}, \ldots, g_{i_1}}_{q_1}, \ldots, \underbrace{g_{i_m}, \ldots, g_{i_m}}_{q_m}),$$

onde $q_1 \geq q_2 \geq \cdots \geq q_m > 0$, $q_1 + q_2 + \cdots + q_m = n$ e os elementos $g_{i_1}, \ldots, g_{i_m}$ são dois a dois distintos. Assim, para descrever a graduação em R diremos que a estrutura de graduação elementar é definida pela upla

$$(q_1, q_2, \ldots, q_m; g_{12}, g_{23}, \ldots, g_{m-1,m}),$$

onde $q_1 + \cdots + q_m = n$ e $g_{12} = g_{i_1}^{-1} g_{i_2}, g_{23} = g_{i_2}^{-1} g_{i_3}, \ldots, g_{m-1,m} = g_{i_{m-1}}^{-1} g_{i_m}$. Além disso, segue que $g_{i,i+1} \cdots g_{j-1,j} \neq e$ para todos $1 \leq i < j \leq m$. Em diversos momentos usaremos essa caracterização de uma graduação elementar.

Lema 4.0.14. *Seja R uma álgebra G-graduada simples de dimensão finita sobre um corpo algebricamente fechado F tal que a ordem de cada subgrupo finito de G é invertível em F. Considere uma decomposição $R = A \otimes B$ onde A é uma álgebra de matrizes com graduação elementar e B é uma álgebra G-graduada de divisão com graduação canônica, conforme o teorema* (3.4.1)*. Denote também $S = supp(A)$ e $H = supp(B)$. Se G é abeliano então $S \cap H = \{e\}$.*

Demonstração. Seja $h \in S \cap H$ e suponha $h \neq e$. Suponha que $(g_1, \ldots, g_n)$ gradua A e $\{r_h \ : h \in H\}$ seja uma base para B. Então, como $h \in S$, existe $E_{ij} \in A$ tal que $deg(E_{ij}) = g_i^{-1} g_j = h$. Como $h \in H$, então considere o elemento básico $r_{h^{-1}} \in B_{h^{-1}}$. Logo, como G é abeliano

$$deg(E_{ij} \otimes r_{h^{-1}}) = g_i^{-1} h^{-1} g_j = e$$

Logo $E_{ij} \otimes r_{h^{-1}} \in R_e = A_e \otimes 1$, onde 1 é a unidade da álgebra B. Mas então

$$E_{ij} \otimes r_{h^{-1}} = \sum_{s,t \ : \ g_s^{-1} g_t = e} \alpha_{st} (E_{st} \otimes r_e)$$

para certos escalares $\alpha_{st} \in F$, não todos nulos. Mas isso é um absurdo pois o conjunto $\{E_{kl} \otimes r_p \ : 1 \leq k, l \leq n \text{ e } p \in H\}$ é base para o espaço vetorial $A \otimes B$. $\square$

4.1 Teorema principal

Sejam G um grupo e R uma F-álgebra G-graduada simples de dimensão finita, onde F é algebricamente fechado e a ordem de cada subgrupo finito de G é invertível em F. Então, pelo teorema (3.4.1) existe um subgrupo finito H de G, um 2-cociclo $\sigma : H \times H \to F^*$, um natural n e uma n-upla $(g_1, \ldots, g_n) \in G^n$ tais que R é G-isomorfa a $C = M_n(F) \otimes F^\sigma[H]$ onde $C_g = Span\{E_{ij} \otimes r_h \ : g_i^{-1} h g_j = g\}$. Nestas condições, dizemos que a tripla $P = (H, \sigma, (g_1, \ldots, g_n))$ é uma **apresentação de** R. Em certos momentos escreveremos R_P no lugar de apenas R para dizer que estamos considerando R com a apresentação P.

Vejamos agora um lema técnico fundamental na demonstração do resultado principal. A menos que seja dito o contrário, uma álgebra graduada simples cumprirá as hipóteses do teorema (3.4.1).

Lema 4.1.1. *Seja R uma álgebra G-graduada simples com apresentação*

$$P = (H, \sigma, (g_1, \ldots, g_n)).$$

As seguintes "mudanças"na apresentação P determinam uma álgebra G-graduada G-isomorfa a R_P:

1. *Dada $\tau \in S_n$, considere nova apresentação $P' = (H, \sigma, (g_{\tau(1)}, \ldots, g_{\tau(n)}))$ de R. Então R_P e $R_{P'}$ são G-isomorfas.*

2. *Fixados $i = 1, \ldots, n$ e $h_0 \in H$, substituir g_i por $h_0 g_i$.*

3. *Para um arbitrário $g \in G$,*

   (a) Substituir H por gHg^{-1},

   (b) Substituir o 2-cociclo σ em H por um 2-cociclo σ^g em gHg^{-1}, onde σ^g é dado por

   $$\sigma^g(gh_1g^{-1}, gh_2g^{-1}) = \sigma(h_1, h_2)$$

   e

   (c) substituir a n-upla $(g_1, \ldots, g_n)$ por $(gg_1, \ldots, gg_n)$.

Demonstração. (1) Defina $\varphi : R_{P'} \to R_P$ por $\varphi(E_{ij} \otimes r_h) = E_{\tau(i),\tau(j)} \otimes r_h$. Observe que φ é linear por construção. Além disso, como $\tau \in S_n$, segue que φ é uma bijeção. Assim, dados $u = E_{ij} \otimes r_h, v = E_{st} \otimes r_g \in R$, se $s \neq j$ então $\tau(s) \neq \tau(j)$ e então $\varphi(uv) = 0 = \varphi(u)\varphi(v)$.

Caso $s = j$, temos

$$\begin{aligned}
\varphi(uv) &= \sigma(h,g)\varphi(E_{it} \otimes r_{hg}) \\
&= \sigma(h,g)E_{\tau(i),\tau(t)} \otimes r_{hg} \\
&= (E_{\tau(i),\tau(j)} \otimes r_h)(E_{\tau(j),\tau(t)} \otimes r_g) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

Portanto φ é um isomorfismo de álgebras. Finalmente,

$$deg(\varphi(E_{ij} \otimes r_h)) = deg(E_{\tau(i),\tau(j)} \otimes r_h) = g_{\tau(i)}^{-1} h g_{\tau(j)} = deg(E_{ij} \otimes r_h).$$

Portanto φ é um G-isomorfismo.

(2) Considere a nova apresentação $P' = (H, \sigma, (g_1, \ldots, g_{i-1}, h_0 g_i, g_{i+1}, \ldots, g_n))$ e defina $\varphi : R_P \to R_{P'}$ por

$$\begin{aligned}
E_{ii} \otimes r_h &\mapsto E_{ii} \otimes r_{h_0} r_h r_{h_0}^{-1}, \\
E_{it} \otimes r_h &\mapsto E_{it} \otimes r_{h_0} r_h, \ \ se\ t \neq i, \\
E_{si} \otimes r_h &\mapsto E_{si} \otimes r_h r_{h_0}^{-1}, \ \ se\ s \neq i, \\
E_{st} \otimes r_h &\mapsto E_{st} \otimes r_h, \ \ se\ s \neq i\ \ e\ t \neq i.
\end{aligned}$$

Observe que φ é linear por construção. Além disso é sobrejetora. De fato, dado $u = E_{st} \otimes r_h \in R$,

- Se $s = i$ e $t = i$ então $\varphi(E_{st} \otimes r_{h_0}^{-1} r_h r_{h_0}) = u$,
- Se $s = i$ e $t \neq i$ então $\varphi(E_{st} \otimes r_{h_0}^{-1} r_h) = u$,
- Se $s \neq i$ e $t = i$ então $\varphi(E_{st} \otimes r_h r_{h_0}) = u$,
- Se $s \neq i$ e $t \neq i$ então $\varphi(E_{st} \otimes r_h) = u$.

Consequentemente φ é sobrejetora e então isomorfismo de espaços vetoriais. Mostremos agora que φ preserva o produto. É necessário verificar apenas nos elementos da base.

Tomemos então $u = E_{pq} \otimes r_h$ e $v = E_{st} \otimes r_g$. Note que se $q \neq s$ então $\varphi(uv) = 0 = \varphi(u)\varphi(v)$. Consideremos então os casos onde $u = E_{ps} \otimes r_h$ e $v = E_{st} \otimes r_g$.

$\underline{p \neq i,\ s \neq i,\ t \neq i}$

$$\begin{aligned} \varphi(uv) &= \sigma(h,g)\varphi(E_{pt} \otimes r_{hg}) \\ &= E_{pt} \otimes r_h r_g \\ &= (E_{ps} \otimes r_h)(E_{st} \otimes r_g) \\ &= \varphi(u)\varphi(v). \end{aligned}$$

$\underline{p = i,\ s \neq i,\ t \neq i}$

$$\begin{aligned} \varphi(uv) &= \sigma(h,g)\varphi(E_{it} \otimes r_{hg}) \\ &= E_{it} \otimes r_{h_0} r_h r_g \\ &= (E_{is} \otimes r_{h_0} r_h)(E_{st} \otimes r_g) \\ &= \varphi(u)\varphi(v). \end{aligned}$$

$\underline{p \neq i,\ s = i,\ t \neq i}$

$$\begin{aligned} \varphi(uv) &= \sigma(h,g)\varphi(E_{pt} \otimes r_{hg}) \\ &= E_{pt} \otimes r_h r_g \\ &= (E_{pi} \otimes r_h r_{h_0}^{-1})(E_{it} \otimes r_{h_0} r_g) \\ &= \varphi(u)\varphi(v). \end{aligned}$$

$\underline{p \neq i,\ s \neq i,\ t = i}$

$$\begin{aligned} \varphi(uv) &= \sigma(h,g)\varphi(E_{pi} \otimes r_{hg}) \\ &= E_{pi} \otimes r_h r_g r_{h_0}^{-1} \\ &= (E_{ps} \otimes r_h)(E_{si} \otimes r_g r_{h_0}^{-1}) \\ &= \varphi(u)\varphi(v). \end{aligned}$$

<u>$p = i,\ s = i,\ t \neq i$</u>

$$\begin{aligned}
\varphi(uv) &= \sigma(h,g)\varphi(E_{it} \otimes r_{hg}) \\
&= E_{it} \otimes r_{h_0} r_h r_g \\
&= (E_{ii} \otimes r_{h_0} r_h r_{h_0}^{-1})(E_{it} \otimes r_{h_0} r_g) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

<u>$p = i,\ s \neq i,\ t = i$</u>

$$\begin{aligned}
\varphi(uv) &= \sigma(h,g)\varphi(E_{ii} \otimes r_{hg}) \\
&= E_{ii} \otimes r_{h_0} r_h r_g r_{h_0}^{-1} \\
&= (E_{is} \otimes r_{h_0} r_h)(E_{si} \otimes r_g r_{h_0}^{-1}) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

<u>$p \neq i,\ s = i,\ t = i$</u>

$$\begin{aligned}
\varphi(uv) &= \sigma(h,g)\varphi(E_{pi} \otimes r_{hg}) \\
&= E_{pi} \otimes r_h r_g r_{h_0}^{-1} \\
&= (E_{pi} \otimes r_h r_{h_0}^{-1})(E_{ii} \otimes r_{h_0} r_g r_{h_0}^{-1}) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

<u>$p = i,\ s = i,\ t = i$</u>

$$\begin{aligned}
\varphi(uv) &= \sigma(h,g)\varphi(E_{ii} \otimes r_{hg}) \\
&= E_{ii} \otimes r_{h_0} r_h r_g r_{h_0}^{-1} \\
&= (E_{ii} \otimes r_{h_0} r_h r_{h_0}^{-1})(E_{ii} \otimes r_{h_0} r_g r_{h_0}^{-1}) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

Portanto φ é, de fato, um isomorfismo de álgebras. Mostremos que tal aplicação preserva a estrutura de graduação. Sejam $s, t = 1, \ldots, n$ tais que $s \neq i$ e $t \neq i$. Então:

$$\begin{aligned} deg(\varphi(E_{ii} \otimes r_h)) &= deg(E_{ii} \otimes r_{h_0} r_h r_{h_0}^{-1}) \\ &= (h_0 g_i)^{-1} h_0 h h_0^{-1} (h_0 g_i) \\ &= g_i^{-1} h g_i \\ &= deg(E_{ii} \otimes r_h). \end{aligned}$$

$$\begin{aligned} deg(\varphi(E_{it} \otimes r_h)) &= deg(E_{it} \otimes r_{h_0} r_h) \\ &= (h_0 g_i)^{-1} h_0 h g_t \\ &= g_i^{-1} h g_t \\ &= deg(E_{it} \otimes r_h). \end{aligned}$$

$$\begin{aligned} deg(\varphi(E_{si} \otimes r_h)) &= deg(E_{si} \otimes r_h r_{h_0}^{-1} \\ &= g_s^{-1} h h_0^{-1} (h_0 g_i) \\ &= g_s^{-1} h g_i \\ &= deg(E_{si} \otimes r_h). \end{aligned}$$

$$\begin{aligned} deg(\varphi(E_{st} \otimes r_h)) &= deg(E_{st} \otimes r_h \\ &= g_s^{-1} h g_t \\ &= deg(E_{st} \otimes r_h). \end{aligned}$$

Portanto φ é um G-isomorfismo e o item (2) está provado.

(3) Defina $\varphi : R_P \to R_{P'}$ por $\varphi(E_{ij} \otimes r_h) = E_{ij} \otimes r_{ghg^{-1}}$. Então nota-se que φ é um isomorfismo de espaços vetoriais. Além disso, sejam $u = E_{ij} \otimes r_h$ e $v = E_{st} \otimes r_p$ tensores

simples em R. Se $j \neq s$ então $\varphi(uv) = 0 = \varphi(u)\varphi(v)$. Se $j = s$ então

$$\begin{aligned}
\varphi(u)\varphi(v) &= (E_{ij} \otimes r_{ghg^{-1}})(E_{jt} \otimes r_{gpg^{-1}}) \\
&= \sigma^g(ghg^{-1}, gpg^{-1})E_{it} \otimes r_{ghpg^{-1}} \\
&= \sigma(h,p)E_{it} \otimes r_{ghpg^{-1}} \\
&= \sigma(h,p)\varphi(E_{it} \otimes r_{hp}) \\
&= \varphi((E_{ij} \otimes r_h)(E_{jt} \otimes r_p)) \\
&= \varphi(uv).
\end{aligned}$$

Usando o item (c) de (3), temos que φ é um G-isomorfismo.

□

Definição 4.1.2. *Os isomorfismos definidos no lema acima são chamados de* ***movimentos básicos*** *de tipos* (1), (2) *e* (3).

Lema 4.1.3. *Seja G um grupo abeliano e F um corpo algebricamente fechado tal que a ordem de cada subgrupo finito de G é invertível em F. Sejam $R = AB$ e $R' = A'B'$ duas F-álgebras G-graduadas simples de dimensão finita, onde A e A' tem graduações elementares definidas pelas uplas*

$$(q_1, \ldots, q_m; g_{12}, \ldots, g_{m-1,m}) \text{ e } (q'_1, \ldots, q'_m; g'_{12}, \ldots, g'_{m-1,m}),$$

respectivamente, enquanto que B e B' são álgebras de divisão, conforme o teorema (3.4.1). *Suponha ainda que R e R' satisfaçam as seguintes condições:*

1. *$A \cong A' \cong M_n(F)$ como álgebras não graduadas;*
2. *Supp B = Supp $B' = H \leq G$ e $B \cong B'$ como álgebras graduadas;*
3. *Existe uma permutação $\sigma \in S_m$ e $h_1, \ldots, h_{m-1} \in H$ tais que $q'_{\sigma(i)} = q_i$ para todo $i = 1, \ldots, m$ e*

$$g_{12} = g'_{\sigma(1),\sigma(2)}h_1, \ldots g_{m-1,m} = g'_{\sigma(m-1),\sigma(m)}h_{m-1}$$

onde $g'_{ij} = g'_{i,i+1} \cdots g'_{j-1,j}$ para todo $i < j$ e $g'_{ij} = (g'_{ji})^{-1}$ para todo $i > j$.

Então R e R' são isomorfas como álgebras G-graduadas.

Demonstração. Pelo teorema (3.4.1), existem dois 2-cociclos $\alpha, \beta : H \times H \to F^*$ tais que $B \cong F^\alpha[H]$ e $B' \cong F^\beta[H]$ como álgebras graduadas. Denote por

$$P = (H, \alpha, (g_1, \dots, g_1, \dots, g_m, \dots, g_m)) \text{ e } P' = (H, \beta, (g'_1, \dots, g'_1, \dots, g'_m, \dots, g'_m))$$

as duas apresentações de R e R' respectivamente. Pelo lema anterior, usando uma permutação τ de S_n conveniente, ao reordenar a upla acima obtendo

$$(g'_{\sigma(1)}, \dots, g'_{\sigma(1)}, \dots, g'_{\sigma(m)}, \dots, g'_{\sigma(m)})$$

obtemos uma nova apresentação P'_τ de R' de tal forma que $R'_{P'}$ é G-isomorfa a $R'_{P'_\tau}$. Assim, podemos supor inicialmente que σ é a permutação identidade e que

$$g_{12} = g'_{12} h_1, \dots, g_{m-1,m} = g'_{m-1,m} h_{m-1}$$

para certos $h_i \in H$, $i = 1, \dots, m-1$. Daí temos que $q'_i = q_i$ para quaisquer $i = 1, \dots, m$.

Obtenha uma nova apresentação de R' substituindo cada entrada g_i (movimentos básicos do tipo (2)) da seguinte maneira:

- $g'_1 \rightarrowtail g''_1 := g'_1$
- $g'_2 \rightarrowtail g''_2 := h_1 g'_2$
- $g'_3 \rightarrowtail g''_3 := h_1 h_2 g'_3$
- $\vdots$
- $g'_m \rightarrowtail g''_m := h_1 h_2 \cdots h_{m-1} g'_m$

Denote tal nova apresentação de R' por $P'' = (H, \beta, (g''_1, \dots, g''_1, \dots, g''_m, \dots, g''_m))$. Pelo lema anterior, $R'_{P'}$ é isomorfa a $R'_{P''}$ como álgebras G-graduadas. O lema fica provado se mostrarmos que R_P é isomorfa a $R'_{P''}$ como álgebras graduadas.

Seja $\theta : B \to B'$ o isomorfismo que existe por hipótese entre as álgebras graduadas B e B'. Defina

$$\begin{array}{rcl} f : R_P & \longrightarrow & R'_{P''} \\ E_{ij} \otimes r_h & \mapsto & E_{ij} \otimes \theta(r_h) \end{array}$$

Note que f é um isomorfismo de álgebras (f é o produto tensorial de isomorfismos, que é um isomorfismo). Resta-nos verificar que f preserva a graduação. Antes disso, observe que para $i = 1, \ldots, m-1$

$$\begin{array}{rcl} (g''_i)^{-1} g''_{i+1} & = & h_1^{-1} h_2^{-1} \cdots h_{i-1}^{-1} (g'_i)^{-1} h_1 h_2 \cdots h_i g'_{i+1} \\ & = & (g'_i)^{-1} g'_{i+1} h_i \\ & = & g'_{i,i+1} h_i \\ & = & g_{i,i+1}. \end{array}$$

Reescrevendo $(g_1, \ldots, g_1, \ldots, g_m, \ldots, g_m) = (a_1, \ldots, a_n)$ e $(g''_1, \ldots, g''_1, \ldots, g''_m, \ldots, g''_m) = (b_1, \ldots, b_n)$, teremos que

$$(a_i)^{-1} a_j = (b_i)^{-1} b_j,$$

para quaisquer $i, j = 1, \ldots, n$. Deste modo,

$$\begin{array}{rcl} deg(f(E_{ij} \otimes r_h)) & = & deg(E_{ij} \otimes \theta(r_h)) \\ & = & (b_i)^{-1} h b_j \\ & = & (b_i)^{-1} b_j h \\ & = & (a_i)^{-1} a_j h \\ & = & (a_i)^{-1} h a_j \\ & = & deg(E_{ij} \otimes r_h) \end{array}$$

e o lema está provado. □

Agora considere a seguinte situação: Sejam R e R' duas F-álgebras G-graduadas simples de dimensão finita tais que o corpo F e o grupo G satisfazem as hipóteses do teorema (3.4.1). Então, podemos escrever $R \cong M_n(F) \otimes F^{\alpha}[H]$ e $R' \cong M_{n'} \otimes F^{\beta}[H']$. Assumindo que G seja abeliano, [19] demonstra que se R e R' satisfazem as mesmas identidades graduadas então os grupos H e H' coincidem. Na verdade esse é um resultado mais geral: se retirada a hipótese de comutatividade de G então ainda se tem $H = H'$. Para este fato, ver [1].

Lema 4.1.4. *Seja G um grupo abeliano e F um corpo algebricamente fechado tal que a ordem de cada subgrupo finito de G é invertível em F. Se duas F-álgebras G-graduadas simples de dimensão finita R e R' satisfazem as mesmas identidades graduadas então R e R' são isomorfas como álgebras G-graduadas.*

Demonstração. Sejam $R = AB \cong A \otimes B$ e $R' = A'B' \cong A' \otimes B'$ duas decomposições nos moldes do teorema (3.4.1), isto é, existem inteiros positivos n e n', subgrupos finitos H e H' de G, um 2-cociclo α em H, outro 2-cociclo β em H' e duas uplas $u = (g_1, \ldots, g_n) \in G^n$ e $v = (g'_1, \ldots, g'_{n'}) \in G^{n'}$, tais que R tem apresentação $P_R = (H, \alpha, u)$ e R' tem apresentação $P_{R'} = (H', \beta, v)$. Note que pelo lema (4.1.1), podemos assumir que

$$u = (\underbrace{g_1, \ldots, g_1}_{q_1}, \ldots, \underbrace{g_m, \ldots, g_m}_{q_m}),$$

com $q_1 \geq q_2 \geq \cdots \geq q_m > 0$, de modo que $q_1 + q_2 + \cdots + q_m = n$ e $g_1, \ldots, g_m$ são distintos; e

$$v = (\underbrace{g'_1, \ldots, g'_1}_{q'_1}, \ldots, \underbrace{g'_{m'}, \ldots, g'_{m'}}_{q'_{m'}}),$$

com $q'_1 \geq q'_2 \geq \cdots \geq q'_{m'} > 0$, de modo que $q'_1 + q'_2 + \cdots + q'_{m'} = n'$ e $g'_1, \ldots, g'_{m'}$ são distintos. Então, A tem graduação elementar definida por $(q_1, q_2, \ldots, q_m; g_{12}, g_{23}, \ldots, g_{m-1,m})$, enquanto que A' tem graduação elementar definida por $(q'_1, q'_2, \ldots, q'_{m'}; g'_{12}, g'_{23}, \ldots, g'_{m'-1,m'})$, onde denotamos $g_{st} = g_s^{-1} g_t$, $1 \leq s, t \leq m$ e $g'_{kl} = (g'_k)^{-1} g'_l$, $1 \leq k, l \leq m'$. Além disso, para quaisquer $1 \leq s < t \leq m$ vale que $g_{s,s+1} \cdots g_{t-1,t} \neq e$. De modo análogo, para quaisquer $1 \leq k < l \leq m'$ vale que $g'_{k,k+1} \cdots g'_{l-1,l} \neq e$.

Defina os seguintes elementos $p'_i s$:

$$p_1 = q_1,\ p_2 = p_1 + q_2,\ \cdots,\ p_{m-1} = p_{m-2} + q_{m-1},\ p_m = p_{m-1} + q_m = n$$

e

$$p'_1 = q'_1,\ p'_2 = p'_1 + q'_2,\ \cdots,\ p'_{m'-1} = p'_{m'-2} + q'_{m'-1},\ p'_{m'} = p_{m'-1} + q_{m'} = n'.$$

Defina também os seguintes polinômios graduados: f e f' pertencentes a $F\langle X\rangle$:

$$f(x_1^e, \ldots, x_{2p_1-1}^e, x_{2p_1}^{g_{12}}, x_{2p_1+1}^e, \ldots, x_{2p_{m-1}-1}^e, x_{2p_{m-1}}^{g_{m-1,m}}, x_{2p_{m-1}+1}^e, \ldots, x_{2n-1}^e, x_{2n}^e) =$$
$$= St_{2q_1-1}(x_1^e, \ldots, x_{2p_1-1}^e)x_{2p_1}^{g_{12}} St_{2q_2-1}(x_{2p_1+1}^e, \ldots, x_{2p_2-1}^e)x_{2p_2}^{g_{23}} \cdots St_{2q_{m-1}-1}(x_{2p_{m-2}+1}^e, \ldots, x_{2p_{m-1}-1}^e)$$
$$x_{2p_{m-1}}^{g_{m-1,m}} St_{2q_m-1}(x_{2p_{m-1}+1}^e, \ldots, x_{2p_m-1}^e)x_{2p_m}^e$$

e

$$f'(x_1^e, \ldots, x_{2p'_1-1}^e, x_{2p'_1}^{g'_{12}}, x_{2p'_1+1}^e, \ldots, x_{2p'_{m'-1}-1}^e, x_{2p'_{m'-1}}^{g'_{m'-1,m'}}, x_{2p'_{m'-1}+1}^e, \ldots, x_{2n'-1}^e, x_{2n'}^e) =$$
$$= St_{2q'_1-1}(x_1^e, \ldots, x_{2p'_1-1}^e)x_{2p'_1}^{g'_{12}} St_{2q'_2-1}(x_{2p'_1+1}^e, \ldots, x_{2p'_2-1}^e)x_{2p'_2}^{g'_{23}} \cdots St_{2q'_{m'-1}-1}(x_{2p'_{m'-2}+1}^e, \ldots, x_{2p'_{m'-1}-1}^e)$$
$$x_{2p'_{m'-1}}^{g'_{m'-1,m'}} St_{2q'_{m'}-1}(x_{2p'_{m'-1}+1}^e, \ldots, x_{2p'_{m'}-1}^e)x_{2p'_{m'}}^e.$$

Afirmação 1. *f não é identidade polinomial graduada para A (e portanto não é para R).*

De fato, usando o argumento de escada,

$$f(E_{11}, E_{12}, \ldots, E_{p_1\ p_1}, E_{p_1\ p_1+1}, E_{p_1+1\ p_1+1}, \ldots, E_{p_2\ p_2}, E_{p_2\ p_2+1}, E_{p_2+1\ p_2+1}, \ldots,$$
$$\ldots, E_{p_{m-1}\ p_{m-1}}, E_{p_{m-1}\ p_{m-1}+1}, E_{p_{m-1}+1\ p_{m-1}+1}, \ldots, E_{nn}, E_{nn}) = E_{1n} \neq 0.$$

Afirmação 2. *f' não é identidade polinomial graduada para A' (e portanto não é para R').*

O argumento é análogo ao da afirmação anterior.

Afirmação 3. $m = m'$

Para provarmos a afirmação, comecemos supondo que $m > m'$. Neste caso, vamos mostrar que f é uma identidade graduada para R', o que é uma contradição com o enunciado. Para tal, devemos tomar elementos arbitrários de R'_e e $R'_{g_{12}}, \ldots, R'_{g_{m-1,m}}$. Mas note que

- R' é G-isomorfa a $M_{n'}(F) \otimes F^\beta[H]$,

- $R'_e = A'_e \cong \underbrace{M_{q'_1}(F)}_{A'_1} \oplus \underbrace{M_{q'_2}(F)}_{A'_2} \oplus \cdots \oplus \underbrace{M_{q'_{m'}}(F)}_{A'_{m'}}$,
- f é multilinear.

Logo podemos tomar, sem perder generalidade, elementos

- $y_1 \otimes 1, \ldots, y_{2p_1-1} \otimes 1, y_{2p_1+1} \otimes 1, \ldots, y_{2p_{m-1}-1} \otimes 1, y_{2p_{m-1}+1} \otimes 1, \ldots, y_{2p_m-1} \otimes 1, y_{2p_m} \otimes 1$ pertencentes a $R'_e \cong A'_e \otimes 1$, com cada y_j pertencente a alguma componente $A'_1, \ldots, A'_{m'}$.
- $y_{2p_1} \otimes b_1 \in R'_{g_{12}}, \ldots, y_{2p_{m-1}} \otimes b_{m-1} \in R'_{g_{m-1,m}}$ com cada um dos $y_{2p_1}, \ldots, y_{2p_{m-1}}$ e $b_1, \ldots, b_{m-1}$ homogêneos em $M_{n'}(F)$ e $F^\beta[H]$ respectivamente.
- Para fins de notação, defina os conjuntos

$$I_1 = \{y_1, \ldots, y_{2p_1-1}\}, I_2 = \{y_{2p_1+1}, \ldots, y_{2p_2-1}\}, \ldots, I_m = \{y_{2p_{m-1}+1}, \ldots, y_{2p_m-1}\}.$$

Diremos que os $2n$ elementos arbitrários acima foram tomados do **tipo 1**.

Assim, $f(y_1 \otimes 1, \ldots, y_{2p_m} \otimes 1)$ assume valor

$$St_{2q_1-1}(y_1 \otimes 1, \ldots, y_{2p_1-1} \otimes 1)(y_{2p_1} \otimes b_1) \cdots St_{2q_m-1}(y_{2p_{m-1}+1} \otimes 1, \ldots, y_{2p_m-1} \otimes 1)(y_{2p_m} \otimes 1) =$$
$$= \underbrace{St_{2q_1-1}(y_1, \ldots, y_{2p_1-1})}_{a_1} y_{2p_1} \cdots \underbrace{St_{2q_m-1}(y_{2p_{m-1}+1}, \ldots, y_{2p_m-1})}_{a_m} y_{2p_m} \otimes b_1 b_2 \cdots b_{m-1} =$$
$$= \underbrace{f(y_1, \ldots, y_{2p_m})}_{\Delta} \otimes b_1 b_2 \cdots b_{m-1}.$$

Então, para alcançar nosso objetivo, basta mostrar-mos que $\Delta = 0$. Dividamos a análise de Δ em dois casos:

1. **Algum dos conjuntos $I_1, \ldots, I_m$ contém dois elementos em componentes distintas:** Neste caso, se tal fato acontece com o bloco I_j então temos

$$St_{2q_j-1}(y_{2p_{j-1}+1}, \ldots, y_{2p_j-1}) = 0$$

pois tais elementos que se repetem aparecem em toda parcela deste fator de f. Então neste caso, $\Delta = 0$.

2. **Caso em que $I_1 \subset A'_{i_1}, \ldots, I_m \subset A'_{i_m}$, para certos índices $i_1, \ldots, i_m \in \{1, \ldots, m'\}$:** Neste caso, como estamos supondo $m > m'$ então dois dos índices $i_1, \ldots, i_m$ devem coincidir, digamos $i_s = i_t$, com $1 \leq s < t \leq m$. Deste modo, se

$$a_s y_{2p_s} \cdots y_{2p_{t-1}} a_t \in A'_{i_s}$$

é não nulo, então deveríamos ter

$$e = deg(a_s y_{2p_s} \cdots y_{2p_{t-1}} a_t) = deg(y_{2p_s}) \cdots deg(y_{2p_{t-1}})$$

(pois $a_s, \ldots, a_t$ são homogêneos de grau e). Logo teríamos

$$g'_{st} = deg(y_{2p_s} \otimes b_s) \cdots deg(y_{2p_{t-1}} \otimes b_{t-1}) = deg(b_s \cdots b_{t-1})$$

Como $b_s \cdots b_{t-1} \neq 0$ (pois B' é álgebra de divisão graduada), então temos que $e \neq g'_{st} \in Supp(B') \cap Supp(A')$, o que contradiz o lema (4.0.14). Portanto, $a_s y_{2p_s} \cdots y_{2p_{t-1}} a_t = 0$, o que implica $\Delta = 0$.

Assim, f é uma identidade polinomial graduada para R', o que é um absurdo. Por um argumento análogo, temos que $m' > m$ não pode ocorrer. Logo $m = m'$ e a afirmação 3 está provada.

Afirmação 4. *$q_i = q'_i$, para todo $i = 1, \ldots, m$.*

Suponha $q_1 > q'_1$. Neste caso, mostraremos que f é identidade graduada para R'. Considere $2n$ elementos arbitrários tomados do *tipo 1*. Mais uma vez, para provarmos que f se anula nesse elementos (e que, portanto, é identidade graduada para R'), basta mostrarmos que

$$\Delta := f(y_1, \ldots, y_{2n}) = St_{2q_1-1}(y_1, \ldots, y_{2p_1-1}) y_{2p_1} \cdots St_{2q_m-1}(y_{2p_{m-1}+1}, \ldots, y_{2p_m-1}) y_{2p_m}$$

é zero. Dividimos em três casos:

1. **Algum dos conjuntos $I_1, \ldots, I_m$ contém dois elementos em componentes distintas:**

2. **Caso em que $I_1 \subset A'_{i_1}, \ldots, I_m \subset A'_{i_m}$, para certos índices $i_1, \ldots, i_m \in \{1, \ldots, m\}$, de forma que dois dos índices $i_1, \ldots, i_m$ coincidam:**

3. **Caso em que $I_1 \subset A'_{i_1}, \ldots, I_m \subset A'_{i_m}$, para certos índices $i_1, \ldots, i_m \in \{1, \ldots, m\}$, de forma que os índices $i_1, \ldots, i_m$ são dois a dois distintos:**

Observe que para mostrar que $\Delta = 0$ nos casos (1) e (2), usa-se o mesmo argumento que usamos na suposição de $m > m'$ (veja que lá não usamos o fato de que $q_1 > q'_1$). Nos resta verificar o caso (3). Note que como $q_1 > q'_1$ então $2q_1 - 1 \geq 2q'_1$. Além disso, $q'_1 \geq \cdots \geq q'_m$. Assim, as matrizes $y_1, \ldots, y_{2p_1-1}$ pertencem a $M_d(F)$, com $d \in \{q'_1, \ldots, q'_m\}$ (têm tamanho máximo $(q'_1)^2$). Pelo teorema de Amitsur-Levitzki,

$$St_{2q_1-1}(y_1, \ldots, y_{2p_1-1}) = 0,$$

o que implica $\Delta = 0$. Daí f seria uma identidade graduada para R', o que é uma contradição. Por um argumento análogo, mostra-se que $q'_1 > q_1$ não pode ocorrer. Portanto $q_1 = q'_1$.

Façamos o caso geral, isto é, suponha que $q_1 = q'_1, \ldots, q_{k-1} = q'_{k-1}$, para certo $2 \leq k \leq m$. Provemos que $q_k = q'_k$. Suponha $q_k > q'_k$. Provemos neste caso que f é uma identidade graduada para R'. Considerando $2n$ elementos arbitrários tomados do tipo 1 e repetidos todos os argumentos, somente nos resta mostrar que

$$\Delta := f(y_1, \ldots, y_{2n}) = St_{2q_1-1}(y_1, \ldots, y_{2p_1-1})y_{2p_1} \cdots St_{2q_m-1}(y_{2p_{m-1}+1}, \ldots, y_{2p_m-1})y_{2p_m}$$

é zero no caso em que $I_1 \subset A'_{i_1}, \ldots, I_m \subset A'_{i_m}$, para certos índices $i_1, \ldots, i_m \in \{1, \ldots, m\}$, de forma que os índices $i_1, \ldots, i_m$ são dois a dois distintos. Observe que se $i_k \geq k$ então as matrizes $y_{2p_{k-1}+1}, \ldots, y_{2p_k-1}$ pertencem a $M_d(F)$ com $d \in \{q'_k, q'_{k+1}, \ldots, q'_m\}$ (têm tamanho máximo $(q'_k)^2$). Então como $2q_k - 1 \geq 2q'_k$, segue por Amitsur-Levitzki que

$$St_{2q_k-1}(y_{2p_{k-1}+1}, \ldots, y_{2p_k-1}) = 0,$$

o que implica $\Delta = 0$. Por outro lado, se $i_k < k$ então algum dos índices $i_1, \ldots i_{k-1}$ é maior do que ou igual a k (uma vez que $i_1, \ldots, i_m$ são distintos). Seja então $i_l \geq k$, para algum $1 \leq l \leq k-1$. Então, as matrizes $y_{2p_{l-1}+1}, \ldots, y_{2p_l-1}$ pertencem a $M_d(F)$ com $d \in \{q'_k, q'_{k+1}, \ldots, q'_m\}$ (têm tamanho no máximo $(q'_k)^2$). Como $q_l \geq q_k > q'_k$ segue que $2q_l - 1 \geq 2q'_k$ e pelo teorema de Amitsur-Levitzki

$$St_{2q_l-1}(y_{2p_{l-1}+1}, \ldots, y_{2p_l-1}) = 0,$$

o que implica $\Delta = 0$. Portanto f é identidade graduada para R, o que é uma contradição.

Mais uma vez, com um argumento análogo mostra-se, no caso geral, que não podemos ter $q'_k > q_k$. Assim a afirmação 4 está provada. Além disso, temos que $n = n'$ e a condição (1) do lema anterior é satisfeita.

Pela observação logo no início do capítulo, temos que os grupos H e H' coincidem. Assim sendo, denotemos por $\{b_h \ : h \in H\}$ a base homogênea de $F^{\alpha}[H]$ e $\{b'_h \ : h \in H\}$ a base homogênea de $F^{\beta}[H]$. Para cada par $g, h \in H$, defina os escalares $\lambda(g,h) = \frac{\alpha(g,h)}{\alpha(h,g)}$ e $\lambda'(g,h) = \frac{\beta(g,h)}{\beta(h,g)}$. Como G é abeliano, para quaisquer $g, h \in H$,

$$b_g b_h = \lambda(g,h) b_h b_g \text{ e } b'_g b'_h = \lambda'(g,h) b'_h b'_g$$

Lembre que podemos escrever o polinômio standard de grau $2q$ do seguinte modo:

$$St_{2q}(x_1, \ldots, x_{2q-2}, x_{2q-1}, x_{2q}) = \sum_{1 \leq i < j \leq 2q} \left(St_{ij}(x_1, \ldots, x_{2q-2}, x_{2q-1}, x_{2q}) - St_{ij}(x_1, \ldots, x_{2q-2}, x_{2q}, x_{2q-1})\right)$$

onde

$$St_{ij}(x_1, \ldots, x_{2q-2}, x_{2q-1}, x_{2q}) = (-1)^{i+j+1} \sum_{\tau \in S_{2q-2}} (-1)^{\tau} x_{\tau(1)} \cdots x_{\tau(i-1)} x_{2q-1} x_{\tau(i)} \cdots x_{\tau(j-2)} x_{2q} x_{\tau(j-1)} \cdots x_{\tau(2q-2)}.$$

Tome arbitrariamente dois elementos $g, h \in H$. Denotando $q := q_1$, defina então o polinômio graduado:

$$St_{2q}^{g,h}(x_1^e,\dots,x_{2q-2}^e,x_{2q-1}^g,x_{2q}^h) = \sum_{1\le i<j\le 2q}\left(St_{ij}(x_1^e,\dots,x_{2q-2}^e,x_{2q-1}^g,x_{2q}^h) - \lambda(g,h)St_{ij}(x_1^e,\dots,x_{2q-2}^e,x_{2q}^h,x_{2q-1}^g)\right).$$

Afirmação 5. *$St_{2q}^{g,h}$ é identidade graduada para R, para $g,h\in H$ fixados.*

Antes de provarmos a afirmação, vamos a um fato: sejam $h\in H$ fixado e índices $1\le s,t\le 2n$ tais que $E_{st}\otimes b_a\in M_n(F)\otimes F^\alpha[H]$ tenha grau h, onde $a\in H$. Então $g_{st}a=h$. Como $a,h\in H$ e H é subgrupo de G, segue que $g_{st}\in H=Supp(B)$. Mas então $g_{st}\in Supp(A)\cap Supp(B)=\{e\}$. Em resumo: os elementos de R_h são combinações lineares de elementos do tipo $E_{st}\otimes b_h$.

Agora, tomemos $2q-2$ elementos em R_e, um elemento em R_g e outro em R_h. Como $St_{2q}^{g,h}$ é multilinear e $R_e=A_e\cong \underbrace{M_{q_1}(F)}_{A_1}\oplus\cdots\underbrace{\oplus M_{q_m}(F)}_{A_m}$, podemos tomar os elementos:

- $y_1\otimes 1,\dots,y_{2q-2}\otimes 1$ em R_e de modo que cada y_k pertença a alguma componente $A_1,\dots,A_m$;
- $y_{2q-1}\otimes b_g\in R_g$ e $y_{2q}\otimes b_h\in R_h$, onde y_{2q-1} e y_{2q} são matrizes em $M_n(F)$ de grau e.

Assim,

$$\begin{aligned}
&St_{2q}^{g,h}(y_1\otimes 1,\dots,y_{2q-2}\otimes 1,y_{2q-1}\otimes b_g,y_{2q}\otimes b_h)\\
&=\sum_{1\le i<j\le 2q}(St_{ij}(y_1\otimes 1,\dots,y_{2q-1}\otimes b_g,y_{2q}\otimes b_h)-\lambda(g,h)St_{ij}(y_1\otimes 1,\dots,y_{2q}\otimes b_h,y_{2q-1}\otimes b_g))\\
&=\sum_{1\le i<j\le 2q}(St_{ij}(y_1,\dots,y_{2q-2},y_{2q-1},y_{2q})\otimes b_gb_h-\lambda(g,h)St_{ij}(y_1,\dots,y_{2q-2},y_{2q},y_{2q-1})\otimes b_hb_g)\\
&=\sum_{1\le i<j\le 2q}(St_{ij}(y_1,\dots,y_{2q-2},y_{2q-1},y_{2q})\otimes b_gb_h-St_{ij}(y_1,\dots,y_{2q-2},y_{2q},y_{2q-1})\otimes b_gb_h)\\
&=\sum_{1\le i<j\le 2q}(St_{ij}(y_1,\dots,y_{2q-2},y_{2q-1},y_{2q})-St_{ij}(y_1,\dots,y_{2q-2},y_{2q},y_{2q-1}))\otimes b_hb_g\\
&=St_{2q}(y_1,\dots,y_{2q-2},y_{2q},y_{2q-1})\otimes b_gb_h\\
&=0
\end{aligned}$$

uma vez que as matrizes $y_1, \ldots, y_{2q-2}, y_{2q}, y_{2q-1}$ pertencem a $M_d(F)$ com $d \in \{q_1', \ldots, q_m'\}$ e $q = q_1 \geq q_1' \geq \cdots \geq q_m'$. Logo a afirmação 5 está provada.

Afirmação 6. *$\lambda(g,h) = \lambda'(g,h)$ para todos $g, h \in H$.*

Suponha que existam $g, h \in H$ tais que $\lambda(g,h) \neq \lambda'(g,h)$. Então vamos mostrar que $St_{2q}^{g,h}$ não é identidade graduada de R', o que contradiz o enunciado e a afirmação 5. Para isso, tome os elementos

$$\underbrace{E_{11} \otimes 1, E_{12} \otimes 1, \ldots, E_{q-1,q} \otimes 1}_{2q-2 \text{ elementos}} \in R_e'$$

e $E_{qq} \otimes b_g' \in R_g'$ e $E_{qq} \otimes b_h' \in R_h'$. Assim,

$$\begin{aligned}
&St_{2q}^{g,h}(E_{11} \otimes 1, E_{12} \otimes 1, \ldots, E_{q-1,q} \otimes 1, E_{qq} \otimes b_g', E_{qq} \otimes b_h') = \\
&= \sum_{1 \leq i < j \leq 2q} \big(St_{ij}(E_{11}, \ldots, E_{q-1,q}, E_{qq}, E_{qq}) \otimes b_g' b_h' - \lambda(g,h) St_{ij}(E_{11}, \ldots, E_{q-1,q}, E_{qq}, E_{qq}) \otimes b_h' b_g'\big) \\
&= \sum_{1 \leq i < j \leq 2q} \left(St_{ij}(E_{11}, \ldots, E_{q-1,q}, E_{qq}, E_{qq}) \otimes b_g' b_h' - \frac{\lambda(g,h)}{\lambda'(g,h)} St_{ij}(E_{11}, \ldots, E_{q-1,q}, E_{qq}, E_{qq}) \otimes b_g' b_h'\right) \\
&= \left(1 - \frac{\lambda(g,h)}{\lambda'(g,h)}\right) \left(\sum_{1 \leq i < j \leq 2q} St_{ij}(E_{11}, E_{12}, \ldots, E_{q-1,q}, E_{qq}, E_{qq})\right) \otimes b_g' b_h' \\
&= \left(1 - \frac{\lambda(g,h)}{\lambda'(g,h)}\right) E_{1q} \otimes b_g' b_h' \neq 0
\end{aligned}$$

o que é uma contradição. Portanto a afirmação 6 está provada.

Afirmação 7. *B e B' são álgebras H-graduadas isomorfas.*

Como H é grupo abeliano finito, fixe uma decomposição de H em um produto direto de grupos cíclicos de ordens $k_1, \ldots, k_t$, respectivamente

$$H = \langle h_1 \rangle_{k_1} \times \cdots \times \langle h_t \rangle_{k_t}.$$

Podemos tomar $b_1, \ldots, b_t \in B$ tais que $deg(b_i) = h_i$ e $b_i^{k_i} = 1$ para todo $i = 1, \ldots, t$. De fato, para índice fixado $1 \leq i \leq t$, considere o elemento b_{h_i}. Temos que $(b_{h_i})^{k_i} = \xi 1$, para algum $0 \neq \xi \in F$. Como F é algebricamente fechado, existe $\eta \in F$ tal que $\eta^{k_i} = \xi^{-1}$. Assim, o elemento $b_i := \eta b_{h_i}$ é tal que $(b_i)^{h_i} = 1$, como queríamos.

Do mesmo modo, tome elementos $c_1, \ldots, c_t \in B'$ tais que $deg(c_i) = h_i$ e $c_i^{k_i} = 1$, para todo $i = 1, \ldots, t$. Afirmamos que os conjuntos

$$T = \{b_i^{j_1} \cdots b_t^{j_t} \ : 1 \leq j_r \leq k_r, r = 1, \ldots, t\}$$

e

$$T' = \{c_i^{j_1} \cdots c_t^{j_t} \ : 1 \leq j_r \leq k_r, r = 1, \ldots, t\}$$

são bases para B e B' respectivamente. De fato, é imediato que T e T' geram B e B'. Mostremos agora que T é linearmente independente. Note que pela decomposição de H,

$$b_i^{j_1} \cdots b_t^{j_t} = b_i^{l_1} \cdots b_t^{l_t} \Longleftrightarrow (j_1, \ldots, j_t) = (l_1, \ldots, l_t).$$

Sendo assim, considere a combinação linear

$$\sum_{(j_1,\ldots,j_t)} \mu_{(j_1,\ldots,j_t)} b_i^{j_1} \cdots b_t^{j_t} = 0. \tag{4.1.1}$$

Observe que cada parcela à esquerda da igualdade acima é homogênea pois é um produto de elementos homogêneos invertíveis não nulos. Além disso, os elementos das parcelas à esquerda de (4.1.1) têm os graus dois a dois distintos. Como $B = \bigoplus_{h\in H} B_g$, segue que $\mu_{(j_1,\ldots,j_t)} = 0$, para quaisquer $j_1, \ldots, j_t$. Um argumento inteiramente análogo mostra que T' é base para B'. Defina a transformação linear $\psi : B \to B'$ dada por $\psi(b_i^{j_1} \cdots b_t^{j_t}) = c_i^{j_1} \cdots c_t^{j_t}$. Observe que ψ é um isomorfismo de espaços vetoriais. Mostremos que ψ preserva o produto. Defina para cada $1 \leq i < t$, o coeficiente $\Gamma_i =$

$[\lambda(h_t, h_i)]^{j_t l_i}[\lambda(h_{t-1}, h_i)]^{j_{t-1} l_i} \cdots [\lambda(h_{i+1}, h_i)]^{j_{i+1} l_i}$. Deste modo,

$$\begin{aligned}
(b_1^{j_1} \cdots \; b_{t-1}^{j_{t-1}} \; b_t^{j_t})(b_1^{l_1} \cdots b_{t-1}^{l_{t-1}} b_t^{l_t}) &= [\lambda(h_t, h_1)]^{j_t l_1} b_1^{j_1} \cdots b_{t-1}^{j_{t-1}} b_1^{l_1} b_t^{j_t} b_2^{l_2} \cdots b_t^{l_t} \\
&= [\lambda(h_t, h_1)]^{j_t l_1}[\lambda(h_{t-1}, h_1)]^{j_{t-1} l_1} b_1^{j_1} \cdots b_{t-2}^{j_{t-2}} b_1^{l_1} b_{t-1}^{j_{t-1}} b_t^{j_t} b_2^{l_2} \cdots b_t^{l_t} \\
&= \vdots \\
&= [\lambda(h_t, h_1)]^{j_t l_1}[\lambda(h_{t-1}, h_1)]^{j_{t-1} l_1} \cdots [\lambda(h_2, h_1)]^{j_2 l_1} b_1^{j_1} b_1^{l_1} b_2^{j_2} \cdots b_t^{j_t} b_2^{l_2} \cdots b_t^{l_t} \\
&= \Gamma_1 b_1^{j_1+l_1} b_2^{j_2} \cdots b_t^{j_t} b_2^{l_2} \cdots b_t^{l_t} \\
&= \vdots \\
&= \Gamma_1 \Gamma_2 b_1^{j_1+l_1} b_2^{j_2+l_2} b_3^{j_3} \cdots b_t^{j_t} b_3^{l_3} \cdots b_t^{l_t} \\
&= \vdots \\
&= \Gamma_1 \Gamma_2 \cdots \Gamma_{t-1} b_1^{j_1+l_1} b_2^{j_2+l_2} \cdots b_t^{j_t+l_t}.
\end{aligned}$$

De modo inteiramente análogo, mostra-se que

$$(c_1^{j_1} \cdots c_{t-1}^{j_{t-1}} c_t^{j_t})(c_1^{l_1} \cdots c_{t-1}^{l_{t-1}} c_t^{l_t}) = \Gamma_1' \Gamma_2' \cdots \Gamma_{t-1}' c_1^{j_1+l_1} c_2^{j_2+l_2} \cdots c_t^{j_t+l_t},$$

onde $\Gamma_i' = [\lambda'(h_t, h_i)]^{j_t l_i}[\lambda'(h_{t-1}, h_i)]^{j_{t-1} l_i} \cdots [\lambda'(h_{i+1}, h_i)]^{j_{i+1} l_i}$, para cada $1 \leq i < t$. Pela afirmação 6 segue que $\Gamma_i = \Gamma_i'$ para todo $1 \leq i < t$ e então ψ preserva o produto. Além disso, é claro que

$$deg(b_i^{j_1} \cdots b_t^{j_t}) = h_1^{j_1} \cdots h_t^{j_t} = deg(c_i^{j_1} \cdots c_t^{j_t}),$$

o que mostra que ψ é um isomorfismo de álgebras que preserva a graduação. Isso prova a afirmação 7. Logo a condição (2) do lema anterior é satisfeita.

Como o polinômio f não é uma identidade graduada para R', então existem $2n$ elementos

- $y_1 \otimes 1, \ldots, y_{2p_1-1} \otimes 1, y_{2p_1+1} \otimes 1, \ldots, y_{2p_{m-1}-1} \otimes 1, y_{2p_{m-1}+1} \otimes 1, \ldots, y_{2p_m-1} \otimes 1, y_{2p_m} \otimes 1$ pertencentes a $R_e' \cong A_e' \otimes 1$, com cada y_j pertencente a alguma componente $A_1', \ldots, A_{m'}'$.

- $y_{2p_1} \otimes b_1 \in R_{g_{12}}', \ldots, y_{2p_{m-1}} \otimes b_{m-1} \in R_{g_{m-1,m}}'$ com cada um dos $y_{2p_1}, \ldots, y_{2p_{m-1}}$ sendo matrizes elementares e cada b_i homogêneos em B' com grau h_i, $i = 1, \ldots, m-1$.

- Para fins de notação, defina os conjuntos

$$I_1 = \{y_1, \dots, y_{2p_1-1}\}, I_2 = \{y_{2p_1+1}, \dots, y_{2p_2-1}\}, \dots, I_m = \{y_{2p_{m-1}+1}, \dots, y_{2p_m-1}\}$$

satizfazendo

$$\begin{aligned} 0 \neq & St_{2q_1-1}(y_1 \otimes 1, \dots, y_{2p_1-1} \otimes 1)(y_{2p_1} \otimes b_1) \cdots St_{2q_m-1}(y_{2p_{m-1}+1} \otimes 1, \dots, y_{2p_m-1} \otimes 1)(y_{2p_m} \otimes 1) \\ &= \underbrace{St_{2q_1-1}(y_1, \dots, y_{2p_1-1})}_{a_1} y_{2p_1} \cdots \underbrace{St_{2q_m-1}(y_{2p_{m-1}+1}, \dots, y_{2p_m-1})}_{a_m} y_{2p_m} \otimes b_1 b_2 \cdots b_{m-1} \end{aligned}$$

o que implica $a_1 y_{2p_1} a_2 \cdots y_{2p_{m-1}} a_m \neq 0$. Escreva

$$y_{2p_1} = E_{i_1 j_1}, y_{2p_2} = E_{i_2 j_2} \dots, y_{2p_{m-1}} = E_{i_{m-1}, j_{m-1}}$$

para certos índices $1 \leq i_1, j_1, \dots, i_{m-1}, j_{m-1} \leq n$. Daí,

$$\begin{aligned} &\underbrace{St_{2q_1-1}(y_1, \dots, y_{2p_1-1})}_{a_1} E_{i_1 j_1} St_{2q_2-1}(y_{2p_1+1}, \dots, y_{2p_2-1}) E_{i_2 j_2} \cdots E_{i_{m-1} j_{m-1}} \\ &\qquad \underbrace{St_{2q_m-1}(y_{2p_{m-1}+1}, \dots, y_{2p_m-1})}_{a_m} \neq 0. \end{aligned}$$

Observe que devemos ter $I_1 \subset A'_{l_1}, \dots, I_m \subset A'_{l_m}$ de modo que os índices $l_1, \dots, l_m$ são uma permutação de $\{1, \dots, m\}$. Seja $\sigma \in S_m$ tal que $\sigma(j) = l_j$

Denote os subconjuntos de números naturais

$$\{1, \dots p_1\}, \{p_1 + 1, \dots, p_2\}, \dots, \{p_{m-1} + 1, \dots, p_m\}$$

por **sub-blocos**. Relembre que a upla

$$(\underbrace{g'_1, \dots, g'_1}_{q_1}, \underbrace{g'_2, \dots, g'_2}_{q_2}, \dots, \underbrace{g'_m, \dots, g'_m}_{q_m})$$

determina a estrutura de graduação de A'. Observe que para $1 \leq k \leq m-1$, se os índices i_k e j_k pertencem a um mesmo sub-bloco, então $h_k = deg(E_{i_kj_k} \otimes b_k) = g_{k,k+1}$, donde teríamos $e \neq g_{k,k+1} \in Supp(A) \cap Supp(B)$, o que é um absurdo. Além disso, para $1 \leq s \leq m-2$ os índices j_s e i_{s+1} devem pertencer a um mesmo sub-bloco. Deste modo, teremos

$$deg(E_{i_1j_1}) = g'_{\sigma(1)\sigma(2)}, deg(E_{i_2j_2}) = g'_{\sigma(2)\sigma(3)}, \ldots, E_{i_{m-1}mj_{m-1}} = g'_{\sigma(m-1),\sigma(m)}$$

donde tiramos que

$$g_{k,k+1} = g'_{\sigma(k),\sigma(k+1)}h_k$$

para $k = 1, \ldots, m$. Isso mostra que R e R' satisfazem as condições do lema anterior. Portanto são G-isomorfas. $\square$

Finalmente, podemos enunciar o teorema principal:

Teorema 4.1.5. *Seja F um corpo algebricamente fechado e G um grupo abeliano tal que a ordem de cada subgrupo finito de G é invertível em F. Sejam $R \cong A \otimes B$ e $R' \cong A' \otimes B'$ duas F-álgebras G-graduadas simples de dimensão finita tais que A e A' são álgebras de matrizes com graduações elementares respectivamente definidas pelas uplas $(q_1, \ldots, q_m; g_{12}, \ldots, g_{m-1,m})$ e $(q'_1, \ldots, q'_{m'}; g'_{12}, \ldots, g'_{m'-1,m'})$, e B e B' são algebras G-graduadas de divisão. Então as seguintes condições são equivalenetes:*

1. *R e R' são G-isomorfas;*

2. *R e R' satisfazem as mesmas identidades graduadas;*

3. *R e R' satisfazem as condições*

   (a) *$A \cong A' \cong M_n(F)$ como álgebras não graduadas;*

   (b) *$supp(B) = supp(B') = H \leq G$ e $B \cong B'$ como álgebras graduadas;*

   (c) *$m = m'$ e existe uma permutação $\sigma \in S_m$ e elementos $h_1, \ldots, h_{m-1} \in H$ tais que $q'_{\sigma(i)} = q_i$ para todo $i = 1, \ldots, m$ e*

$$g_{12} = g'_{\sigma(1)m\sigma(2)}h_1, \ldots, g_{m-1,m} = g'_{\sigma(m-1),\sigma(m)}h_{m-1}$$

onde $g'_{ij} = g'_{i,i+1} \cdots g'_{j-1,j}$ *para quaisquer* $1 \leq i < j \leq m$ *enquanto que* $g'_{ji} = (g'_{ij})^{-1}$.

Demonstração. Segue pelos dois lemas anteriores. $\square$

Referências Bibliográficas

[1] ALJADEFF, E.; HAILE, D. **Simple G-graded algebras and their polynomial identities**. AMS, Volume 336, Número 4, p. 1749-1771. 2014.

[2] AMITSUR, S. A.; LEVITZKI, J. **Minimal identities for algebras** Proc. Amer. Math. Soc. 1, p. 449-463, 1950.

[3] BATHURIN, Y.; ZAICEV, M.; SEHGAL, S. K. **Finite dimensional graded simple algebras**. Matematicheskii Sbornik, 199:7 21-40. Russia: 2008.

[4] BATHURIN, Y.; ZAICEV, M. **Group gradings on matrix algebras**. Canad. Math. Bull. 241:2 499-508, 2002.

[5] BELOV, A. **On non-Specht varieties**. Fundam. Prikl. Mat. 5, vol. 1, p. 47-66, 1999.

[6] BELOV, A. **Counterexamples to the Specht problem**. Mat. Sb. 191, vol. 3, p. 13-24, 2000. Tradução em Inglês em: Sbornik Mathematics 191, vol. 3, p. 329-340, 2000.

[7] BRESAR, M. **Introduction to noncummutative algebra**. Springer International Publishing. 2014.

[8] DEHN, M. **"Uber die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme**. (Em Alemão) Mathematische Annalen 85, p. 184-194, 1922.

[9] DOMOKOS, M. **New identities for 3×3 matrices**. Li. Multilin. Algebra 38, p. 207-213, 1995.

[10] DRENSKY, V. **Free Algebras and PI-Algebras: Graduate Courses in Algebra**. Springer-Verlag , Singapore, 1999.

[11] DRENSKY, V. **A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0**. Algebra i Logika 20, p. 282-290, 1981 (Rússia). Traduação em Inglês em Algebra and Logic 20, p. 188-194, 1981.

[12] DUMMIT, D. S.; FOOTE, R. M. **Abstract Algebra**, 3^a ed. Wiley , Estados Unidos, 2004.

[13] GIAMBRUNO, A.; ZAICEV, M. **Polynomial Identities and Asymptotic Methods**, Amer. Math. Soc. 122, 2005. Surveys and Monographs, Vol. 122, 2005.

[14] GRISHIN, A. V. **Examples of T-spaces and T-ideals in Characteristic 2 without the Finite Basis Property**. Fundam. Prikl. Mat. 5, vol. 1, p. 101-118, 1999.

[15] HERSTEIN, I. N. **Noncommutative Rings**. Wiley, Nova York, 1968.

[16] JACOBSON, N. **Basic Algebra II**. Freeman, Nova York, 1989.

[17] KAPLANSKY, I. **Rings with a polynomial identity** Bull. Amer. Math. Soc. 54, p. 496-500, 1948.

[18] KEMER, A. **Identities of associative algebras**. American Mathematical Society., Ser. 2, vol. 148, p. 65-71, 1991.

[19] KOSHLUKOV, P.; ZAICEV, M. **Identities and isomorphisms of graded simple algebras**. Linear Algebra and its Applications, 432 (2010), 3141-3148.

[20] LAM, T. Y. **A first course in noncommutative rings**. Springer ,1991.

[21] MACÊDO, D. L. S. **PI-equivalências em Álgebras Matriciais**. Dissertação de mestrado, Campina Grande, 2015.

[22] OKHITIN, S. V. **On varieties defined by two-variables identites**, Moscov. Gos. Univ., Moscou, 1986.

[23] PASSMAN, D. S. **The algebraic structure of group rings**. Pure and Applied Mathmatics, Wiley, Nova York-Londres-Sydney, 1977.

[24] PASSMAN, D. S. **Infinite crossed products**. Pure and Applied Mathmatics, vol. 135, Academic Press, Boston, MA 1989.

[25] SCHIGOLEV **Examples of T-spaces with an infinite basis**. Math. Sb. 191, volume 3, p. 143-160, 2000. Tradução em Inglês em: Sbornik Mathematics, 191, vol. 3, p. 459-476, 2000.

[26] SILVA, D. D. P. **Álgebras graduadas e identidades polinomiais graduadas**. Dissertação de mestrado, UNICAMP 2007.

[27] WAGNER, W. **Über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme**. (Em Alemão) Mathematische Annalen 113, 528-567, 1936.